2013-09

Technological advancements in EW: a way forward for Royal Saudi Naval Force

Aladaili, Aabdulaziz A.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TECHNOLOGICAL ADVANCEMENTS IN EW: A WAY FORWARD FOR ROYAL SAUDI NAVAL FORCE

by

Aabdulaziz A. Aladaili

September 2013

Thesis Co-Advisors: David Jenn
Edward Fisher

Second Reader: Joshua Green

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
TECHNOLOGICAL ADVANCEMENTS IN EW: A WAY FORWARD FOR ROYAL SAUDI NAVAL FORCE

5. FUNDING NUMBERS

6. AUTHOR(S) Aabdulaziz A. Aladaili

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release;distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT

The modern battlefield has become exceedingly complex and technology driven. It is signified by highly sophisticated surveillance systems thereby resulting in reduced time for decision making, execution of orders and conduct of operations. This reduced response time is essentially due to non-availability of requisite enemy data and presentation of information extracted from that data in a less understandable format. Modern electronic warfare (EW) systems are designed to process such information automatically to facilitate decision makers in better understanding of the battlefield situation and making quick decisions, thereby allowing more response time to the warfighter on the scene.

Saudi Arabia, the thirteenth-largest nation in the world, is located in an oil rich region and shares its borders with Iraq, Kuwait, Bahrain, Oman, Yemen, Jordan and the United Arab Emirates. This region has been in a state of conflict for many decades. The Iraq–Iran war, the Iraqi occupation of Kuwait, Operation Enduring Freedom and Desert Shield, Iran's ambitions of becoming a nuclear power, and Syria's civil war are examples of recent and on-going conflicts. As a regional power, Saudi Arabia has her economic interests coupled with regional security. With more than 2000 kilometers of coastline to defend, Saudi Arabia faces a challenge keeping economically vital sea lines of communication open for the export of crude oil and other petroleum products. All these factors demand a high degree of operational readiness by Royal Saudi Armed forces, especially the Royal Saudi Naval Force.

14. SUBJECT TERMS RSNF, Electronic Warfare, RADAR, Gap Analysis, Technical Aspects of EW, C4I, Saudi Arabia	**15. NUMBER OF PAGES** 95
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release;distribution is unlimited

TECHNOLOGICAL ADVANCEMENTS IN EW: A WAY FORWARD FOR ROYAL SAUDI NAVAL FORCE

Aabdulaziz A. Aladaili
Lieutenant, Royal Saudi Naval Force
B.S, King Fahad Naval Academy, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRONIC WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Aabdulaziz A. Aladaili

Approved by: Dr. David Jenn
Thesis Co-Advisor

Mr. Edward Fisher
Thesis Co-Advisor

Lt. Col. Joshua Green
Second Reader

Dr. Dan Boger
Chair, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The modern battlefield has become exceedingly complex and technology driven. It is signified by highly sophisticated surveillance systems thereby resulting in reduced time for decision making, execution of orders and conduct of operations. This reduced response time is essentially due to non-availability of requisite enemy data and presentation of information extracted from that data in a less understandable format. Modern electronic warfare (EW) systems are designed to process such information automatically to facilitate decision makers in better understanding of the battlefield situation and making quick decisions, thereby allowing more response time to the warfighter on the scene.

Saudi Arabia, the thirteenth-largest nation in the world, is located in an oil rich region and shares its borders with Iraq, Kuwait, Bahrain, Oman, Yemen, Jordan and the United Arab Emirates. This region has been in a state of conflict for many decades. The Iraq–Iran war, the Iraqi occupation of Kuwait, Operation Enduring Freedom and Desert Shield, Iran's ambitions of becoming a nuclear power, and Syria's civil war are examples of recent and on-going conflicts. As a regional power, Saudi Arabia has her economic interests coupled with regional security. With more than 2000 kilometers of coastline to defend, Saudi Arabia faces a challenge keeping economically vital sea lines of communication open for the export of crude oil and other petroleum products. All these factors demand a high degree of operational readiness by Royal Saudi Armed forces, especially the Royal Saudi Naval Force.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAED	Advance airborne expendable decoy
AEC	Advance electronic company
AEW&C	Airborne early warning and control
AWACS	Airborne warning and control system
AGPO	Angle gate pull-off
AOA	Angle of arrival
AAW	Anti-air warfare
ARM	Anti-radiation missile
AOC	Association of old crows
BMD	Ballistic missile defense
BVR	Beyond visual range
CSS	Central security service
CMCP	Coalition maritime campaign plan
CTF	Combined Task Force
C4I	Command, control, communications, computers and intelligence
C4ISR	Command, control, communications, computers, intelligence, sensors and reconnaissance
CMWS	Common missile warning system
C2	Communication and command
CW	Continuous wave
CM	Cruise missile
CV Rx	Crystal video receiver
DoD	Department of defense

DEWS	Digital electronic warfare system
DF	Direction finding
ERP	Effective radiated power
EM	Electromagnetic
EMC	Electromagnetic compatibility
EME	Electromagnetic environment
EMS	Electromagnetic spectrum
EA	Electronic attack
ECM	Electronic counter measures
ECCM	Electronic counter-counter measures
ELINT	Electronic intelligence
EOB	Electronic order of battle
EP	Electronic protection
EPM	Electronic protection measures
ES	Electronic Support
ESM	Electronic support measure
EW	Electronic warfare
EMD	Engineering manufacturing and development
FMCW	Frequency modulated continuous wave
FRP	Full rate production
GCC	Gulf Cooperation Council
HSN	High speed network
HVU	High value unit
HOJ	Home on jam

IFF	Identification friend or foe
IED	Improvised explosive device
IR	Improvised infra-red
IW	Information warfare
IRCM	Infra-red counter measure
ICMS	Integrated combat management system
KACST	King Abdulaziz city for science and technology
KSA	Kingdom of Saudi Arabia
LCS	Littoral combat ship
LORO	Lobe on receiver only
LPI	Low probability of intercept
MSO	Maritime security operations
MENA	Middle East and North Africa
MSBU	Military system business unit
MODA	Ministry of Defense and Aviation
MBET	Missile borne ECM technology
NEWAC	NATO electronic warfare advisory committee
NCW	Network centric warfare
NCIR	Non-cooperative intercept receiver
OE	Operational environment
OIC	Organization of Islamic Countries
OPEC	Organization of Petroleum Exporting Countries
OEM	Original equipment manufacturer
PLA	People liberation army

POL	Petroleum, oil, lubricants
POI	Probability of intercept
RCS	Radar cross section
RWR	Radar warning receiver
RGPO	Range gate pull-off
RISTA	Reconnaissance, intelligence, surveillance and target acquisition
RPV	Remotely piloted vehicle
RSADF	Royal Saudi air defense force
RSAF	Royal Saudi air force
RSLF	Royal Saudi land forces
RSNF	Royal Saudi Naval Force
SATCOM	Satellite communication
SNEP	Saudi naval expansion program
SIGINT	Signal intelligence
SNR	Signal to noise ratio
SOF	Special operation forces
SRBOC	Super rapid bloom of chaff
SEAD	Suppression of enemy air defense
TBM	Tactical ballistic missile
TBMBJ	Tactical ballistic missile borne jammer
TOJ	Track on jam
UAV	Unmanned aerial vehicle
VGPO	Velocity gate pull-off
VCD	Vertical converge diagram

WAN	Wide area network
WML	World Muslim League
WTO	World Trade Organization

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my advisors, Professor David Jenn and Mr. Ed Fisher, for their continuous guidance throughout the conduct of this research. Their professionalism and expertise directly contributed to making this research a success.

I would also like to extend my special thanks to the Department of Information Sciences for equipping me with the level of knowledge required to complete this research over the past 24 months. They taught me the necessary tools to succeed and to carry on with future endeavors in my life.

Also, I would like to thank the first woman in my life and the biggest love in my life, the woman who was holding me the most closely in her thoughts, my mother, Seetah Aljarad. Furthermore, gratitude is extended to my father and my idol, Maj. Gen. Abdullah S. Aledaili, for his continual guidance and priceless advice.

Finally, I would like to thank my family for their support and being considerate during this whole research process. I appreciate their understanding and help for encouraging me to put my time in completing this important degree milestone instead of demanding long vacations to tour the most beautiful attractions of the United States of America.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Saudi Arabia is progressing as an economic as well as a military power in the Middle East. The region has been in a state of flux during the past several decades and has a very volatile security situation. The Royal Saudi Armed Forces in general and Royal Saudi Naval Force (RSNF), in particular, shoulder a heavy responsibility for guarding national interests from any threat. This mission cannot be accomplished without equipping the RSNF with essential military hardware. The modern battlefield has become exceedingly complex and technology driven. The availability of modern surveillance systems may result in better situational awareness of military decision makers in the execution of orders and conduct of operations. Command and control (C2) systems perform complex computing functions based on the input received from various surveillance sensors, including electronic warfare, to give the tactical picture of the combat area. These systems are designed to process information automatically to enable quick decision making, thereby allowing more response time for the warfighter on the scene. Modern C2 systems are challenged in performing their functions by adversary electronic warfare (EW). At the same time, EW is used by friendly forces to ensure that C2 systems are able to function robustly and complete necessary missions. Modern combat cannot take place ignoring EW capabilities.

With every passing day, nonmilitary factors are becoming increasingly important and militaries of the world will be required to respond to a variety of crises, requiring better integration of military actions with the nonmilitary elements of national power. In order to accomplish the diverse range of potential missions effectively and efficiently, militaries will heavily depend on their EW assets. Saudi Arabia is no exception. Enhancing the EW capabilities of the RSNF will be a force multiplier.

A. POLITICAL SITUATION

The political system in Saudi Arabia is unique and has a tremendous effect on decision making at strategic levels. Funding of any new project, therefore, depends upon all the intricacies of the political dynamics of the country. Armed forces of the Kingdom

are under tremendous pressure to improve due to their increased role and responsibility, coupled with the high economic stakes.

Saudi Arabia is a center of influence in the region. The Kingdom of Saudi Arabia (KSA) is a major political and economic force in the region. The Kingdom has a huge income from its vast oil resources and sponsors the poorer developing Arab nations. These factors have helped the Kingdom to increase its influence in the region. Furthermore, as the birthplace of Islam, its religious and cultural influence has been apparent in the broader Muslim world. Other civilized nations of the world that depend upon imported oil, including the United States and China, have a strong relationship with the Kingdom. The security of these increased economic interests and influence in the region has increased the scope of operation for Royal Saudi Armed Forces.

The system of government in the Kingdom of Saudi Arabia is a monarchy. The monarch must be a direct male descendant of the founder, King Abdul Aziz Saudi Arabia, under a "Basic Law of Government" decreed by King Fahad in 1992 [1]. This law is based on the guidance provided by the Quran and Sunnah. The declared purpose of the Saudi State is the advancement and protection of Islam.

The King is also the prime minister of the country and has the executive powers along with being the head of state. The King is assisted by a Majlis ash Shura (Consultative Assembly) for legislation. Despite this unique monarchical political structure, the Saudi Arabia Government has always been supportive of the well-being of its people. During the multiple "Arab Spring" uprisings of 2010 and 2011, Saudi Arabia was not affected seriously. There were a very few small demonstrations by the minority Shia community; however, the country remained stable as a whole. King Abdullah is generally popular. In response he announced packages of housing, salary and education worth upwards of $100 billion in early 2011 [2].

The Basic Law provides for the creation of a Consultative Council. People may approach "The King's court" for any complaint or injustice. Every individual has the right to address the public authorities in all matters affecting him/her. The government seeks opinions from people of various walks of life through a variety of means, such as

the Ulema, the council of ministers, the shura, the business community, citizens and the armed forces for any decision making in the Kingdom.

While the King and senior princes maintain the ancient Arabian tradition of the majlis—a form of open assembly—in their palaces, to give ordinary citizens the right to present petitions or air grievances, popular political participation has always been restricted and parties are banned. In October 2003, the government announced plans to set up municipal elections with half the seats up for election. The plan was given a cautious welcome by the public, but critics of the regime saw it as merely a token gesture [3].

King Abdullah has introduced many reforms, and Saudi society is opening to the world. Joseph A. Kechichian in [4] concludes:

> In the few years since he acceded to the throne on August 1, 2005, King Abdulla bin abdul Aziz has instituted far reaching reforms that, by general recognition, altered the face of the kingdom. Among the significant changes that were introduced were: fundamental reforms concerning judiciary; launching a national dialogue mechanism that allowed Saudi citizens to engage each other in addressing issues that concerned society; holding interfaith dialogues that culminated in July 2008 Madrid conference; establishing a brand new body to select the monarch and his Heir Apparent from among the sons and grandsons of the founder; introducing unprecedented bureaucratic transformations to manage the religious establishment, including the appointment of a new chairman for the Supreme Judicial Council; making changes within the commission for the Promotion of Virtue and Prevention of Vice; appointing a woman as Deputy Education Minister and authorizing the women to serve in the Majlis al-Shurah …. who sensed the time was long past for a fundamental socio political evolution, in which his own yearnings matched those of his subjects.

B. ECONOMIC SITUATION

Military budgets are prone to getting cut during times of fiscal crisis. Acquisition of new systems, especially sophisticated ones, directly depends upon the prevailing economic situation in the country. Saudi Arabia has an oil-based economy with strong government controls over major economic activities. It possesses about 17% of the world's proven petroleum reserves, ranks as the largest exporter of petroleum, and plays a

leading role in OPEC. The petroleum sector accounts for roughly 80% of budget revenues, 45% of GDP, and 90% of export earnings [5].

Saudi Arabia is encouraging the growth of the private sector in order to diversify its economy and to employ more Saudi nationals. Diversification efforts are focusing on power generation, telecommunications, natural gas exploration, and petrochemical sectors. Over five million foreign workers play an important role in the Saudi economy, particularly in the oil and service sectors, while Riyadh is struggling to reduce unemployment among its own nationals. Saudi officials are particularly focused on employing its large youth population, which generally lacks the education and technical skills the private sector needs. Riyadh has substantially boosted spending on job training and education, most recently with the opening of the King Abdallah University of Science and Technology—Saudi Arabia's first co-educational university. As part of its effort to attract foreign investment, Saudi Arabia acceded to the World Trade Organization (WTO) in December 2005 after many years of negotiations. The government has begun establishing six "economic cities" in different regions of the country to promote foreign investment and plans to spend $373 billion between 2010 and 2014 on social development and infrastructure projects to advance Saudi Arabia's economic development [5].

Saudi Arabia’s economic interests are coupled with regional security. Saudi Arabia has 2,640 kilometers of coastline—nearly 1,800 kilometers along the Gulf of Aqaba and the Red Sea and the remainder along the Persian Gulf. Saudi Arabia claims a territorial sea of 12 nautical miles and a contiguous zone of 18 nautical miles, as well as some small islands, seabed, and subsoils beyond the 12-nautical-mile limit [6]. The RSNF has to remain prepared to defend the maritime interests of the nation and to deter aggression. Keeping the sea lines of communication (SLOCs) open is vital for the economy due to the export of crude oil and other petroleum products. All these factors demand a high degree of operational readiness for the Royal Saudi Armed Forces and especially for the RSNF due to the preponderance of maritime interests.

C. REGIONAL SECURITY SITUATION

Saudi Arabia is an important international stakeholder in issues related to the Middle East. Saudi Arabia is thirteenth largest nation in the world by land mass and is located in an oil rich region. Saudi Arabia shares its borders with Iraq, Kuwait, Bahrain, Oman, Yemen, Jordan, Qatar and the UAE [5]. The region has been in a virtual state of conflict for many decades. The Iraq–Iran war, the Iraqi occupation of Kuwait, Operations Desert Storm and Enduring Freedom, Iran's ambitions of becoming a nuclear power, Syria's civil war and the continuing tensions and conflicts with regard to Israel are examples of recent and continuing conflicts. Saudi Arabia is a regional power, and Saudi economic interests are coupled with regional security.

Although the Royal Saudi Armed Forces are continually modernized with state-of-the-art ships, aircraft, artillery, weapons and sensors, the nation remains quite vulnerable to conventional attack from regional powers like Iran and Iraq. Saudi Arabia has been the beneficiary of a protective U.S. security umbrella, yet it did not traditionally allow U.S. forces inside the Kingdom. However, after the invasion of Kuwait by Saddam Hussein, some 500,000 US troops were allowed into the Eastern Province and Northern border of Saudi Arabia, along with a smaller number of U.S. military personnel elsewhere in the Kingdom. At the Kingdom's request, these troops were moved to other Gulf Cooperation Council (GCC) countries by the time of the 2003 U.S.-led invasion of Iraq [7].

Saudi Arabia has long been a strong advocate of the Palestinian cause and has demanded the withdrawal of Israel back behind its 1967 pre-Six Day War borders. Saudi Arabia, being a leader of the Muslim world, feels obliged to criticize the U.S. policy towards the ongoing Arab–Israeli conflict. The Kingdom's foreign policy makers have always faced a challenge in insulating the Kingdom–U.S. relationship from the Palestine–Israel issue. Despite mostly friendly long-term relations with the U.S., Saudi Arabia feels threatened by Israel's regional stance and possible aspirations. Saudi Arabia has a traditional rivalry with Iran due to her hegemonic regional designs and Shiite identity. Figure 1 offers a map of Saudi Arabia showing all the regional security players.

Figure 1. Saudi Arabia map (from Google Maps).

In recent times the fundamental shift from war fighting to war prevention, the shift to conducting military operations short of war or military operations other than war, the growing asymmetric nature of conflict, and the ever changing regional security conditions have created a greater demand for acquisition of EW resources. EW equipment can help to prevent the situation from escalating beyond desired levels by providing a comprehensive and timely awareness of situations, so that politicians and commanders can determine appropriate reactions and implement them while the situation is still manageable. This can only be realized with the help of a very powerful infrastructure of electronic warfare facilities, command and control centers, communication links, computers and displays. This theme is also validated by U.S. Army EW doctrine FM 3-36 [8]:

> Commanders employ and integrate their unit's capabilities and actions within their operational environment to achieve a desired end state. Through analyzing their operational environment, commanders understand how the results of friendly, adversary, and neutral actions may impact that

> end state. During military operations, both friendly and enemy commanders depend on the flow of information to make informed decisions. This flow of information depends on the electronic systems and devices used to communicate, navigate, sense, store, and process information.

D. THE KINGDOM'S ROLE IN THE REGION

Saudi Arabia's foreign policy is based on its need to maintain the market for petroleum products and its role as the guardian of Islam's two holiest places located within its borders, Mecca and Medina. Saudi Arabia's policies play a central role in the policy making of the GCC and the Organization of Petroleum Exporting Countries (OPEC). Saudi Arabia has been a leader in the formation of the World Muslim League (WML) and the Organization of Islamic Countries (OIC). The OIC has its secretariat within the Kingdom in Jeddah and is represented by 57 Muslim states. Its purpose is to "strengthen solidarity and cooperation among member states" [9].

Saudi Arabia also enjoys strong relations with world powers like the U.S.., Japan and China. Saudi Arabia has been struggling to diversify its petroleum market and extend its influence beyond the GCC. Saudi Arabia has managed to diversify its trade and hence its influence. Currently, Japan, China, the U.S., the Republic of Korea, India and Singapore are leading importers of Saudi products. Although Saudi Arabia has been a long-term ally of the U.S. in the region and will likely continue to be so in the foreseeable future, it also maintains very good relations with emerging powers like China and India.

Today, oil supplies about 40% of the world's energy and 95% of its transportation energy. As a result, those who own the lion's share of the reserves of this precious energy source are in the driver's seat of the world economy, and their influence is steadily growing. Since the 1930s the Middle East has emerged as the world's most important source of energy and the key to the stability of the global economy. This region produces 37% of the world's oil and 18% of its gas [10]. Because of the world's dependence on imported oil, Saudi Arabia will continue to be a relevant player in regional and world security in the years to come.

E. RSNF FORCE STRUCTURE

All Saudi conventional forces are organized under the Ministry of Defence and Aviation (MODA) to defend the Kingdom against any external aggression. The RSNF is an operational force of MODA. Another force, the Saudi Arabian National Guard, is responsible for maintaining the internal stability of the Kingdom.

The Royal Saudi Naval Forces, sometimes also referred to as the Royal Saudi Navy (RSN), has its main headquarters located in Riyadh. It has four major branches: Administration, Operations, Intelligence, and Logistics, similar to those of the Army and Air Force. The RSNF is further divided operationally into the western fleet with headquarters at Jeddah on the Red Sea and the eastern fleet with headquarters at Al-Jubayl on the Arabian Gulf. The Marine regiment is organized as an infantry regiment and has a separate command. The Arabian Gulf Division has bases at Dammam, Ras-Tanura, and Al-Qatif, plus a naval aviation element. The Red Sea Division has bases at Haql, Al Wajh, and Yanbu [11].

The RSNF sought guidance from the verse of The Holy Qur'an in setting up its mission,

وهو الذي سخر البحر لتأكلوا منه لحماً طرياً وتستخرجوا منه حليه تلبسونها وترى الفلك }
{مواخر فيه لتبتغوا من فضله ولعلكم تشكرون

"And He Who has subjected to you the sea that you may eat there from fresh flesh and may take forth ornaments which you wear. And thou see the ships ploughing through it, that you may seek His bounty and that you may be grateful."

What distinguishes the naval forces from other branches of the armed forces is its ability to exist and diffuse in forward locations far from the regional borders of the state. This forward deployment is a historical and constant objective of naval forces. Naval forces perform many missions that contribute to attaining national security in its broad concept. Missions may include deterrence of attacks, promotion of regional stability and

readiness for quick responses to any developing crisis at the right time. The RSNF mission is also derived from these guiding principles and is reproduced here:

> Saudi naval forces play economic Facilities Protection tasks at sea and the protection of commercial, military, and civil convoys and securing the country's exports and imports in addition to assist civil authorities in evacuation and rescue operations during disasters and crises. [12]

F. ORGANIZATION OF THESIS

This thesis is organized into four chapters including this chapter.

Chapter I: Introduction. This chapter gives general information regarding the political, economic situation in Saudi Arabia, the impact of ongoing turmoil in the region on stability, Saudi Arabia's role in the region, the RSNF current force structure and its mission.

Chapter II: Literature Review. This chapter will provide a review of the EW environment, technologies, definitions and current trends.

Chapter III: Technical Aspects of EW. This chapter describes the technical aspects of EW, the inter-relationships of various EW elements in a broader perspective and derivation of radar, jamming and POI equations.

Chapter IV: Capability Gap Analysis. This chapter will analyze the current EW capabilities of the Kingdom, will provide an analysis of threats against the Kingdom, and will discuss what EW upgrades that are needed to neutralize the threats effectively.

Chapter V: Current Technological Trends. This chapter will conclude the argument and set some recommendations for decision makers based on the findings. Areas requiring further research will also be highlighted. Budgetary issues, if any, will also be discussed to assist leadership in decision making.

Chapter VI: Summary and Conclusion. This chapter will summarize the argument and conclude the thesis.

G. OBJECTIVES

The purpose or this research is to analyze the security environment in the region and the local political situation, research modern trends in EW technologies, examine the RSNF capability gaps, analyze budgetary conditions and recommend a way forward with an acquisition strategy to fill the gaps. This research shall help RSNF decision makers to acquire EW sensors and integrated systems which will improve situational awareness and thus shorten the decision making cycle in a high tempo operational environment.

II. LITERATURE REVIEW

Victory in the combat zone depends on the degree of real-time knowledge available regarding the enemy's movements and/or intended actions. This knowledge is gathered during peace time as well as with real-time intelligence gathered during hostilities using various electronic sensors. This knowledge is necessary for commanders to plan operations and exercise control during various stages of the conflict. Real-time knowledge also helps commanders to update and modify plans continuously and issue orders to execute different contingencies based on the combat situation. In all such situations, EW systems play the role of the eyes and ears of the commander. Efficacy of EW systems in the combat zone is now a proven fact. During the Gulf War of 1991, strike aircraft were normally not permitted to conduct air operations unless protected by enemy air defense suppression aircraft such as the EA-6B and EF-111. These aircraft were equipped with transmitters to disrupt or "jam" radar equipment used by enemy surface-to-air missiles or antiaircraft artillery systems [13].

Today forces have been exposed to the versatile aspects of the modern operational environment. Electronic warfare systems support is vital to operational effectiveness in a hostile electronic environment. Militaries are, therefore, forced to acquire EW systems in order to prepare for the challenges of the modern battlefield.

A. EW ENVIRONMENT

Electronic systems form the brain of many weapons and sensors employed in modern warfare. These systems provide information to firing platforms regarding target detection, tracking, designation, fire control solution, navigation and motion control for kinetic weapons. Communication and other information networks also consist of electronic systems. The effective use or denial of use of these electronics can contribute decisively to the outcome of any conflict. Efficacy of electronic warfare systems will, therefore, remain a relevant discussion topic in any operational context. The operational environment is a composite of the conditions, circumstances, and influences that affect the employment of EW capabilities and on the decisions of the commander [14].

As mentioned earlier, Saudi Arabia shares its borders with Iraq, Kuwait, Bahrain, Oman, Yemen, Jordan, Qatar and the UAE [5]. The region has been in a state of conflict for many decades. The Iraq–Iran war, Iraq's occupation of Kuwait, Operations Desert Shield/Desert Storm, Enduring Freedom and Iraqi Freedom, Iranian ambitions of becoming a nuclear power, and Syria's civil war are examples of recent or on-going conflicts. Saudi Arabia is a regional power and has her economic interests coupled with regional security. The current security environment demands a higher degree of readiness than is currently the case.

In addition to these territorial borders, Saudi Arabia has a long coastline to defend from any aggression. Keeping the sea lines of communication open is vital for the country's economy due to the high volume of export activity involving crude oil and other petroleum products. A well-equipped RSNF in itself will be a stabilizing factor in the region. EW capabilities and technologies will help RSNF in this regard and assist RSNF in preventing situations or potential crises from escalating beyond manageable levels as well as provide a comprehensive and timely awareness of situations. This information will enable politicians and commanders to determine appropriate reactions and implement them while the situation is still current. This capability requires a developed infrastructure of electronic warfare facilities, command and control centers, communication links, computers and displays.

B. EW BENEFITS

Electronic warfare can be portrayed as electronic combat, which includes operational philosophy, strategy, and doctrine. EW technologies make use of the electromagnetic spectrum (EMS), which includes radio and radar, infrared, optical, and ultraviolet frequencies, to gain control of the EM environment and deny the enemy the capacity to use it to his advantage. The benefit of electronic warfare must ultimately be expressed in terms of combat mission success, such as gaining more intelligence without detection, servicing more targets, improving protection of the nation's own forces, securing EW environment dominance, generating more combat missions for a given force size, and providing more effective combat management. Because electronic warfare

capabilities have a significant price tag, EW must demonstrate a greater benefit than would be provided by a larger force without EW at the same total cost.

As highlighted earlier, superior and effective use of the EMS has become vital for the success of any military operation within the context of modern warfare. EW capabilities are not only necessary for offensive operations but have become a mandatory requirement for the effective defense of a nation's own assets. Most notably, missile and improvised explosive device (IED) threats can be countered by suitably employing electronic warfare technologies, such as jamming systems, anti-radiation missiles and electronic intelligence (ELINT) systems.

C. EW CLASSIFICATION

Electronic warfare is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. As illustrated in Figure 2, electronic warfare consists of three divisions: electronic attack, electronic protection and electronic warfare support [15].

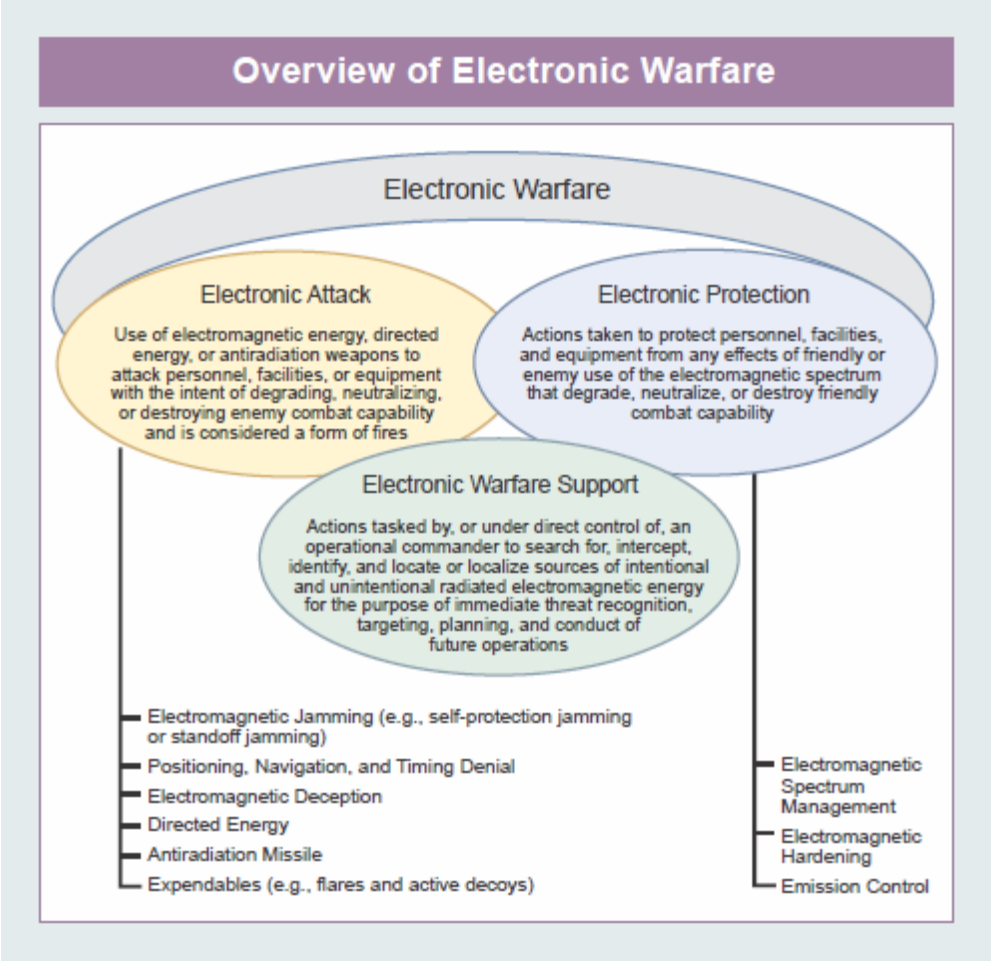

Figure 2. EW classification. (From [15]).

D. PRINCIPAL ACTIVITIES AND KEY TERMS RELATED TO EW

EW is an important capability that can advance desired military, diplomatic, and economic objectives or, conversely, impede undesirable ones. In a military application, EW provides the means to counter, in all battle phases, hostile actions that involve the electromagnetic (EM) spectrum- from the beginning when enemy forces are mobilized for an attack, through to the final engagement [16].

The key terms and principal activities of EW are summarized briefly in the following subsections. All of the information regarding the following activities and terms have been retrieved from [15], unless otherwise cited.

1. Electromagnetic Compatibility

Electromagnetic compatibility (EMC) is the ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environment (OE) without suffering unacceptable degradation or causing unintentional degradation because of EM radiation or response.

2. Electromagnetic Deception

EM deception is the deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability.

3. Electromagnetic Hardening

EM hardening consists of actions taken to protect personnel, facilities, and equipment by filtering, attenuating, grounding, bonding, blanking, and shielding against the undesirable effects of EM energy. EM hardening is an electronic protection (EP) activity.

4. Electronic Masking

Electronic masking is the controlled radiation of EM energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy ES measures/signal intelligence (SIGINT) without significantly degrading the operation of friendly systems.

5. SIGINT

The distinction between ES and SIGINT is delineated by purpose, scope, and context. ES assets are tasked by operational commanders to search for, intercept, identify,

and locate or localize sources of intentional or unintentional radiated EM energy. In contrast, SIGINT assets are tasked by the Director, National Security Agency (NSA)/Chief, Central Security Service (CSS) or understanding or temporary SIGINT operational tasking authority by an operational commander.

6. ESM or ES

According to the Institute of Electrical and Electronics Engineers, the Electronic Support Measure (ESM) or Electronic Support (ES) is "that division of EW involving actions taken to search for, intercept, locate, record, and analyze radiated electromagnetic energy for the purpose of exploiting such radiations in support of military operations . . .. Thus, ESM provides a source of information required to conduct electronic countermeasures (ECM) or Electronic Protection Measures (EPM), electronic counter-counter measures (ECCM) or Electronic Attack (EA), threat detection, warning, avoidance, target acquisition, and homing" [17].

7. ECM or EA

Tactical or strategic operational methods of using electronic technologies to deceive, disrupt, jam or negate the effectiveness of opposing electronic systems and techniques is called ECM/EA [18].

8. ECCM OR EPM

Ways to defeat an enemy's ECM against own electronic systems and actions taken to ensure our own effective use of electromagnetic radiations [18].

9. Jamming

EM jamming is the deliberate radiation, re-radiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EMS, and with the intent of degrading or neutralizing the enemy's combat capability.

10. Look-Through

This is a technique used during jamming or being jammed to monitor the jamming emission or victim signal. It causes irregular interruption for extremely short periods of time. When being jammed, the technique allows for observing or monitoring of a signal during interruptions in the jamming signal [19].

E. EW TECHNIQUES

EW technology is progressing rapidly due to the increased reliance on electronic sensors. EM energy offers unlimited opportunities and vulnerabilities that can be exploited for military operations. Although new equipment and new tactics will continue to be developed, the physical characteristics of EM energy will never change. Therefore, basic activities of EW will remain more or less the same despite variation in hardware and tactics [15].

Much of this technology is highly classified. However, there are generally known techniques that can be employed to make effective use of the EMS. The information below is extracted from relevant chapters of the Royal Navy's *'EW Principles' Student Study Guide* taught at Royal Navy Maritime Warfare School, HMS Collingwood [20] unless otherwise specified. Various techniques used for ESM, ECM and ECCM are listed below. While the terms ESM, ECM, and ECCM are no longer addressed within U.S. joint doctrine and publications, the terminology is still common within industry and with other nations. ESM can be loosely translated as electronic warfare support (ES), ECM as electronic attack (EA), and ECCM as electronic protection (EP).

1. ESM

The basic role of ESM receivers is to detect, classify and report the presence of any electronic signal within a designed frequency band. Some of the techniques used for direction finding (DF) and frequency measurement are appended below:

a. Amplitude comparison technique (8 port digital)

b. Phase comparison technique (multi linear phase array)

c. Time of arrival DF in conjunction with other sensors like GPS

d. Use of Multi Delay Line Instantaneous Frequency Measurement Receiver

2. ECM

All ECM activities are aimed at negating the effective use of the EMS by the enemy electronic systems. Frequently used mature techniques are as follows:

- ***Passive ECM Techniques***

Passive techniques include the use of chaff and reflective decoys to confuse radars and avoidance detection by employing stealth technology features in system design or by following a flight profile outside the vertical coverage diagram (VCD) of the radar (e.g., low level).

- ***Active ECM Techniques***

ECM active techniques may include noise jammers, transponder jammers, false target generators, electronic decoys, Range Gate Pull-Off (RGPO), Angle Gate Pull-Off (AGPO), Velocity Gate Pull-Off (VGPO), home on jam (HOJ) missiles and anti-radiation missiles (ARMs).

3. ECCM OR EPM

ECCM is that subdivision of EW in which measures are taken to defeat an enemy's ECM effort against own electronic warfare systems and actions taken to ensure own effective use of electromagnetic radiations. Some of the techniques used are as follows.

- ***Antenna Features***

There are number of techniques which can be employed by radar antenna to minimize enemy ECM effort. These antenna techniques include polarization agility, lobe on receiver only (LORO), multiple lobing rate, track on jam (TOJ), side lobe blanking, side lobe suppression/cancellation and higher antenna gain.

When a non-coherent jammer transmits, only that part of the signal which is correctly polarized enters the radar receiver. Very little jamming signal will enter the receiver if radar has its plane of polarization orthogonal with respect to the jammer.

Lobing rate information can be denied to amplitude modulation jammers and inverse gain jammers if radar transmits a common beam and only uses multiple beams for the receiver. Some amplitude modulation jammers succeed in causing tracking radar break lock by sweeping very slowly (less than the actual lobing rate).

Angle tracking systems can detect any oscillations caused by amplitude modulation jammers. The radar lobing rate can be altered to damp the oscillation out. This technique is called multiple lobing rate.

In the case when a radar operator feels that radar is being jammed by a self-protection jammer, he can switch off the transmitter and angle track the jammer through the jamming signal being transmitted by the jammer. This technique is called track on jam.

Noise and clutter signals can enter the radar receiver through the side lobes and display as if they are present in the main lobe. Stand off or support jammers take advantage of this fact. In order to cancel the returns received through side lobes, an active side lobe cancellation circuit is used [21].

- ***Transmitter Features***

Electronic protection or ECCM techniques for transmitters includes frequency agility, frequency diversity, burn through range and PRF jittering.

Frequency agility is a technique used by radar transmitters where radar can change its frequency by at least twice per pulse. Random frequency agility will render spot jamming and sweep jamming ineffective forcing the jammer to operate in barrage mode which requires tremendous power to be effective. Frequency agility also helps to increase the maximum effective range of the radar and remove range ambiguities for Low PRF systems.

Frequency diversity is another technique where radar can quickly change band to render spot, sweep or barrage jamming ineffective. As most of the transmitter components are frequency or wavelength specific, the amount of frequency diversity is normally very limited.

Burn through range is the distance beyond which a self-protection jammer cannot obscure the target due to higher skin returns than the jamming signal. Burn through range can be achieved by increasing the radar power output while the antenna is pointing at the jammer. The concept of burn through range is covered in more detail in section C of the next chapter [21].

III. TECHNICAL ASPECTS OF EW

Modern warfare systems such as radars, communication sets, weapon control and guidance systems and displays are comprised of electronic components. Each system has unique electronic characteristics vulnerable to electronic attacks. EW, therefore, is aimed at negating or at least reducing the effectiveness of enemy systems and assisting one's own forces in positive identification of friendly assets and enemy assets. Both of these tasks are accomplished primarily by manipulating various technical characteristics of the electronic components, which in turn are basic building blocks of the larger military systems such as radars, communication equipment, jammers, radios, actuators, data processing assemblies or guidance and control circuits. This chapter covers the technical aspects of these major electronic warfare systems.

A. RADAR

Radar stands for RAdio Detection and Ranging. The basic purpose of radar includes target detection, determination of the target's range, bearing, elevation, velocity and identification of target type and purpose. Radars normally operate in the upper half of the radio spectrum (> 1 MHz). The portion of the electromagnetic spectrum used for various radars is shown in Figure 3.

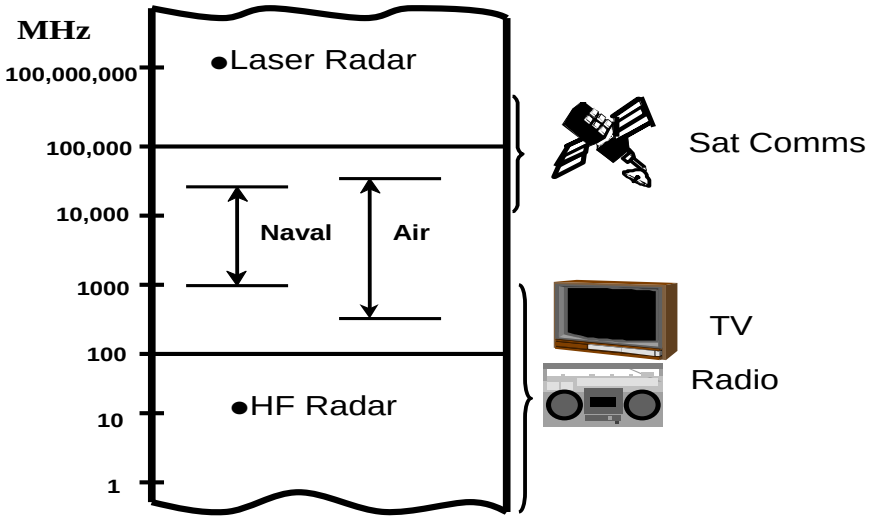

Figure 3. The portion of the EM spectrum used for radar. (From [20]).

Radar can be classified as primary or secondary radar based on transmitted signal and received signal. The main types of primary radar include continuous wave (CW), pulse modulated and frequency modulated continuous wave (FMCW) radars. CW radar applications in a naval environment are limited to Doppler navigation, ship docking, weapon fusing, and target illumination. Pulse modulated radars have variety of naval operational uses such as long-range early warning, surveillance, target indication, tracking/fire control and navigation. FMCW radars are used in some missile fire control systems and as a method of reducing detection by using very low power signals for navigation radars [22].

B. RADAR RANGE EQUATION

The electronic principle on which radar operates is very similar to the principle of sound-wave reflection. Radar uses electromagnetic energy pulses to detect, track and identify a target. The EM energy is transmitted to and reflected from the target object. A small portion of the reflected energy (echo) returns to the radar set. Radar sets use the echo to determine the direction and distance of the reflecting object based on the speed of EM energy and the time required for an echo to return. Modern radar can extract widely more information from a target's echo signal than its range. But the calculation of the range is one of its most important functions.

The radar range equation provides a theoretical means of calculating the maximum range of a radar. If a radar transmits a power P_T from an isotopic (omni-directional) antenna, then the power per unit area (or power density) at a distance R from the transmitting aerial is equal to the transmitted power divided by the surface area of a sphere of radius R is,

$$S_i = \frac{P_T}{4\pi R^2} \tag{1}$$

Radar sets use a directional antenna to focus the transmitted power in a particular direction. The directional gain, *G*, of an antenna is defined as:

$$G = \frac{\textit{Maximum}\text{ power per unit solid angle directional aerial}}{\text{Power per unit solid angle isotropic aerial with same power input}}$$

If the antenna produces a beam of solid angle Ω then G can be redefined as:

$$G = \frac{P_T / \Omega}{P_T / 4\pi} = \frac{4\pi}{\Omega} \quad (2)$$

Applying the antenna gain to the power density gives the power density at distance R from a directional angle of gain G, and we get

$$P_D = \frac{P_T}{4\pi R^2} G \quad (3)$$

At the distance R, a target will reflect a proportion of the incident energy. The amount of power reflected will depend on the incident power density and the effective radar cross sectional area of the target denoted by σ. The power reflected by the target is:

$$\frac{P_T}{4\pi R^2} G\sigma \quad (4)$$

This power is re-radiated in all directions; thus the returning power density at the radar aerial is the reflected power divided by $4\pi R^2$. Power density at the receiving antenna

$$S_r = \frac{P_T G\sigma}{4\pi R^2 4\pi R^2} \quad (5)$$

The amount of power gathered by the receiving antenna P_R, is given by the received power density multiplied by the effective aperture area of the receiving antenna A_e

$$P_R = \frac{P_T G \sigma}{4\pi R^2 4\pi R^2} A_e \quad (6)$$

The half power beamwidth of an antenna is defined approximately by

$$\theta_B = \frac{\lambda}{D} \quad (7)$$

where λ is the wavelength and D is the diameter of antenna aperture. This can be applied separately to the vertical and horizontal planes. In the case where they are all equal, the effective solid angle into which the power of the antenna lobe is directed is

$$\Omega_A = (\theta_B)^2 = \frac{\lambda^2}{D^2} \quad (8)$$

Compared to the solid angle of 4π *steradians* into which a non-directional isotropic antenna radiates its power, the above equation represents a concentration of power, i.e. gain, which is equal to the ratio of the solid angles.

Substituting (8) into (2) gives

$$G = \frac{4\pi}{(\theta_B)^2} = \frac{4\pi D^2}{\lambda^2} \quad (9)$$

Therefore,

$$G = \frac{4\pi A}{\lambda^2} \quad (10)$$

The gain of a practical antenna is less than the ideal value given in (10) and can be rewritten as

$$G = \frac{4\pi\rho A}{\lambda^2} \quad (11)$$

where ρ is the antenna efficiency. Therefore

$$A_e = \rho A \quad (12)$$

and

$$A_e = \frac{G\lambda^2}{4\pi} \quad (13)$$

If the same antenna is used for transmission and reception Equations (6) and (13) can be combined to give

$$P_R = \frac{P_T G^2 \lambda^2 \sigma}{(4\pi)^3 R^4_{\max}} \quad (14)$$

The maximum range of the radar $R_{\max}$ is achieved when the power input to the receiver P_R, has dropped to the lowest level which the receiver is capable of detecting. This is known as the Minimum Detectable Signal, $S_{\min}$

$$S_{\min} = \frac{P_T G^2 \lambda^2 \sigma}{(4\pi)^3 R^4_{\max}} \quad (15)$$

Re-arranging to give an expression for $R_{\max}$

$$R_{\max} = \left(\frac{P_T G^2 \lambda^2 \sigma}{(4\pi)^3 S_{\min}} \right)^{1/4} \quad (16)$$

Finally, we must take into account any losses. Let $L_s = L_t L_r L_a$ be the system loss factor due to losses which are present in the system or in its operating environment. L_t and L_r are the losses on the transmit and receive sides, respectively. L_a is the atmospheric loss. Then [22]

$$R_{\max} = \left(\frac{P_T G_t G_r \lambda \sigma}{(4\pi)^3 \ (\mathrm{S/N})_{\min} L_t L_r L_a} \right)^{1/4} \quad (17)$$

The radar equation is a good source to analyze the tradeoffs in order to improve detection performance. If we look at each part of the radar equation, we can control certain parameters. Increasing the peak transmitter power, the gain of the transmitting antenna and the area of the receiving antenna and reducing the acceptable minimum detectable signal all increase the maximum detection range. However, this is the basic radar equation. Many other factors like detection performance and signal-to-noise ratio (SNR) have not been considered.

We know that thermal noise power in a bandwidth B_n is

$$N = kT_s B_n \quad (18)$$

where

T_s = Total System Noise Temperature

B_n = Noise bandwidth of the receiver

k = Boltzmann's constant (1.38×10^{-23} [J K^{-1}])

To consider noise in this equation, we divide the left side by N and the right side by kT_sB_n. The SNR is

$$\frac{S}{N}=\frac{PG^2\lambda^2\sigma G_p}{(4\pi)^3R^4kT_sB_nL_s} \quad (19)$$

A processing gain factor G_p has been included in the numerator.

In order to get radar information for all bearings, it is necessary to rotate the antenna beam continuously. To be sure of getting an echo from a target, it is necessary to ensure that the beam sweeps at a required rate. For most radar applications, it is an advantage to have as many pulse hits per sweep as possible within the constraints of scanning at a reasonable rate. The returns from multiple targets can be integrated, which provide a processing gain. If the number of hits per scan is n then

$$G_p = nE(n) \quad (20)$$

where:

n = Number of hits (pulses) per second

$E(n)$ = Integration efficiency ($0 \le E_i \le 1$)

Thus if a series of returns is added together the echo power will add, whereas the noise power will not. This gives rise to an improvement in SNR and thus detection range. In some systems, losses in the processing circuitry and the use of non-coherent integration make the improvement factor somewhat lower than the maximum value n that can be achieved.

The final form of the radar range equation considering integration efficiency can be represented as [20]

$$\frac{S}{N} = \frac{PG^2\lambda^2 n\mathrm{E}(n)\,\sigma}{(4\pi)^3\,R^4 k T_s B_n L_s} \quad (21)$$

C. EW RADAR JAMMING EQUATION

ECM can be either jamming or deception. The objective of ECM is to reduce or suppress the effectiveness of enemy defense systems and their relevant weapons systems through soft kill actions such as confusion, distraction, deception or seduction [22]. Active ECM is commonly called jamming, and the calculations of ECM signal in the radar compared to the target signal in the radar commonly refer to the jamming-to-signal ratio (JSR). The term jamming refers to any ECM transmission, whether deception or concealment. Concealment is normally called noise or noise jamming.

Active ECM or jamming against hostile radars may be employed for self-protection or in support of any friendly unit. Support or escort ECM is usually through noise jamming. The SNR at the output of the radar receiver is represented by Equation(21).

Then maximum target detection range from the radar is

$$R_{\max} = \left(\frac{P_T G_t G_r \lambda \sigma}{(4\pi)^3 (S/N)_{\min} L_s k T_s B_r} \right)^{1/4} \quad (22)$$

where $(\mathrm{S/N})_{\min}$ is the minimum signal to noise power ratio for detection.

The jammer power in the radar receiver, spread over a band width B_j (usually larger than the radar receiver bandwidth B_r) is:

$$J = \frac{P_j G_j G_{rJ} \lambda^2 B_r}{(4\pi)^3 R_j^2 L_j B_j} \quad (23)$$

where

P_j = transmitted jammer power

G_j = jammer antenna gain

G_{rJ} = radar antenna gain in the direction of the jammer

R_j = distance of the jammer from the radar

L_j = jammer transmission loss

The jamming equation for a self-protection jammer and a support/escort jammer can be derived separately.

1. Self-protection jammer

For a self-protection jammer, $R = R_j$ and $G_{rj} = G_t = G_r$. Hence, the effective radiated power (ERP) of radar is $\frac{P_t G_t}{L_t}$ and the jammer ERP is $ERP_j = \frac{P_j G_j}{L_j}$. We have intentionally ignored atmospheric loss L_a due its negligible effect. Hence,

$$\frac{J}{S} = \frac{ERP_t 4\pi R_j^2 B_r}{ERP_j \sigma B_r} \quad (24)$$

and a self-screening range R_{jss} can be derived,

$$R_{jss} = \sqrt{\frac{ERP_t B_j \sigma S}{ERP_j 4\pi BJ}} \quad (25)$$

If $\frac{J}{S} = K$, a constant depending upon jamming technique, the $\frac{S}{J} = \frac{1}{K}$.

Replacing this figure in previous equation, the self-screening range of the jammer becomes [22]

$$R_{jss} = \sqrt{\frac{ERP_t B_j \sigma}{ERP_j 4\pi BK}} \quad (26)$$

It can be deduced that more jammer power will be required to achieve self-screening range for targets of higher RCS.

2. Mutual protection jammer

For a mutual protection jammer, $G_{rj} = G_{SLL}$. By assuming that $G_r = G_t$, the burn through range (BTR) of the jammer $R_{t\max j}$ can be given by

$$R_{t\max j} = \sqrt{\frac{ERP_r B_t \sigma R_j^2}{ERP_j 4\pi B_r (S/N)_{\min} G_{SLL}}} \quad (27)$$

The ratio ρ of the detection range in jamming conditions with respect to clear conditions can be derived from Equations (22) and (27):

$$\rho = \frac{R_{t\max j}}{R_{\max-\text{clear}}} = \left[\frac{(4\pi)^2 N R_j^2 B_j}{ERP_j B_r G_r \lambda^2 G_{SLL}} \right]^{1/4} \quad (28)$$

This shows that ρ is increasing with short wavelengths, low side lobe level (SLL) and high radar processing gain. Hence a compromise has to be made between the ERP of the jammer and the frequency for various jamming roles.

D. INTERCEPT RECEIVER

One of the most important tasks of EW is to detect the signal from an unknown transmitter and analyze its parameters, such as frequency, angle of arival (AOA), pulse width and amplitude and pulse repetition frequency for identification purposes. This task is normally carried out by intercept receivers, and the information collected is referred to as ELINT.

In order to detect any incoming signal by an intercept receiver would require an infinite bandwidth which is not possible in reality. Therefore, ESM suites and radar warning receivers (RWRs) consist of number of receivers with small bandwidths to enhance the probability of detection or probability of intercept (POI). Several directional antennas are used to increase the sensitivity of the receiver and enhance receiver ability to measure AOA more accurately.

Intercept receivers require high sensitivity, high dyanmic range and wider bandwidth. Intercept receiver characteristics are related to its functions of interception, recognition and measurement. Intercept system parameters can be capitilized to enhance performance of a specific function at the cost of compromising another one. If we want to design an intercept receiver with high probability of intercept then we will be compromising on the measurement function. To increase the POI, the bandwidth needs to be wide, hence compromising the accuracy of the measurement. Major characteristics of an inercept receiver include POI, sensitivity, dynamic range, coverage band, analysis bandwidth, unusual environment performance, dense environment performance, single pulse performance, multiple simultaneous signal performance and processor/signal sorter requirement [23].

The maximum intercept range (R_I) is given by [24]:

$$R_{I_{\max}} = \sqrt{\frac{P_{cw} G_t G_r \lambda^2}{(4\pi)^2 S_I}} \quad (29)$$

where

P_{cw} = CW power of the emitter

G_t = Emitter antenna gian

G_r = Intercept receiver gain

and

$$S_I = kT_oF_IB_I\left(SNR_I\right) \quad (30)$$

is the sensitivity. The receiver has a noise figure of F_I, a bandwidth B_I, and SNR_I is the SNR at the receiver input. T_o = 290^0 K is the standard temperature. If the emitter is within the maximum intercept range, then an intercept is possible. The POI is discussed next.

E. PROBABILITY OF INTERCEPT

The POI is a measure of the chance of picking up an unknown signal within range of the receiver [21]. POI is a key performance feature of EW surveillance and reconnaissance systems. It relates to the probability of two or more parametric "window functions" such as scanning antennas, sweeping or stepping receivers and frequency agile emitters [23].

EW systems have to deal with increasing complexity and density of the electromagnetic environment, multi-mode emitters, high and low ERPs, increased signal agilities, complex scan and fleeting emissions. Low probability of intercept (LPI) emitters have emerged as a critical POI issue due to the asymmetric nature of threats. EW receiving systems, therefore, have become EW suites which provide situational awareness, protection and ELINT capabilities. EW system designers are being pushed more and more towards architectures that deliver single pulse or pulse burst capabilities [23].

The non-cooperative intercept receiver (NCIR) analysis is similar to the radar received power calculation, but with unpredictable transmitter properties. In other words, the optimum parameters for intercepting and detecting the transmitter signal may not be known.

The POI of a single pulse for a frequency scanning receiver such as a superhetrodyne can be represented mathematically as

$$POI = \frac{\alpha}{D}$$

where

POI = POI (single pulse)

α = Receiver Intermediate Frequency (IF) bandwidth

D = Total receiver frequency scanning rate

The POI of "wide open" receivers such as the crystal video receiver (CV Rx) for a single pulse is 100% [21].

F. A CLASSIC EW SCENARIO

Figure 4 illustrates a classic EW scenerio that shows the interaction of mulitiple EW components. The radar is an emitter that can be detected by the intercept receiver, which then gives the data to the aircraft that can launch a missile. The aircraft is equipped with a jammer that can degrade the radar's performance and impede the detection, tracking and targeting of the missile. The system parameters determine the various detection and burn through ranges. The system specifications are crucial in how an EW network will perform.

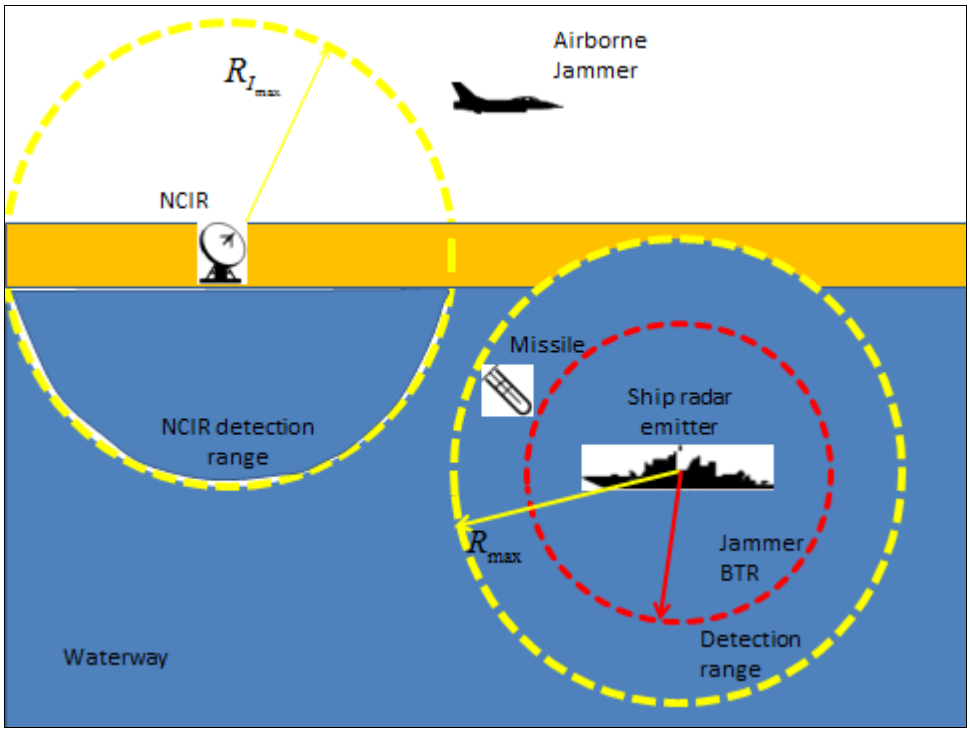

Figure 4. Classic EW scenario.

IV. CAPABILITY GAP ANALYSIS

This EW capabilities gap analysis is based on the understanding of expected war fighting functions of the armed forces of Saudi Arabia and the capabilities required to address potential enemy EW threats within the joint operational environment. This gap analysis can also guide selection of improved EW platforms and systems, and integration of new systems with existing legacy systems.

The first logical step is to identify the needed effects from EW functions and how these functions can be employed most effectively. In today's era of technology, EW capabilities can be applied from air, sea, land and space. The major consideration again will be generation of desired effects involving various levels of detection, denial, deception, disruption, degradation, protection and destruction and the EW system carrying platforms. A variety of other factors like own and enemy electronic order of battle (EOB), operational concepts, equipment employed and users of the equipment remain relevant. All factors combined can be referred to as the Electromagnetic Environment, as shown in Figure 4 [15].

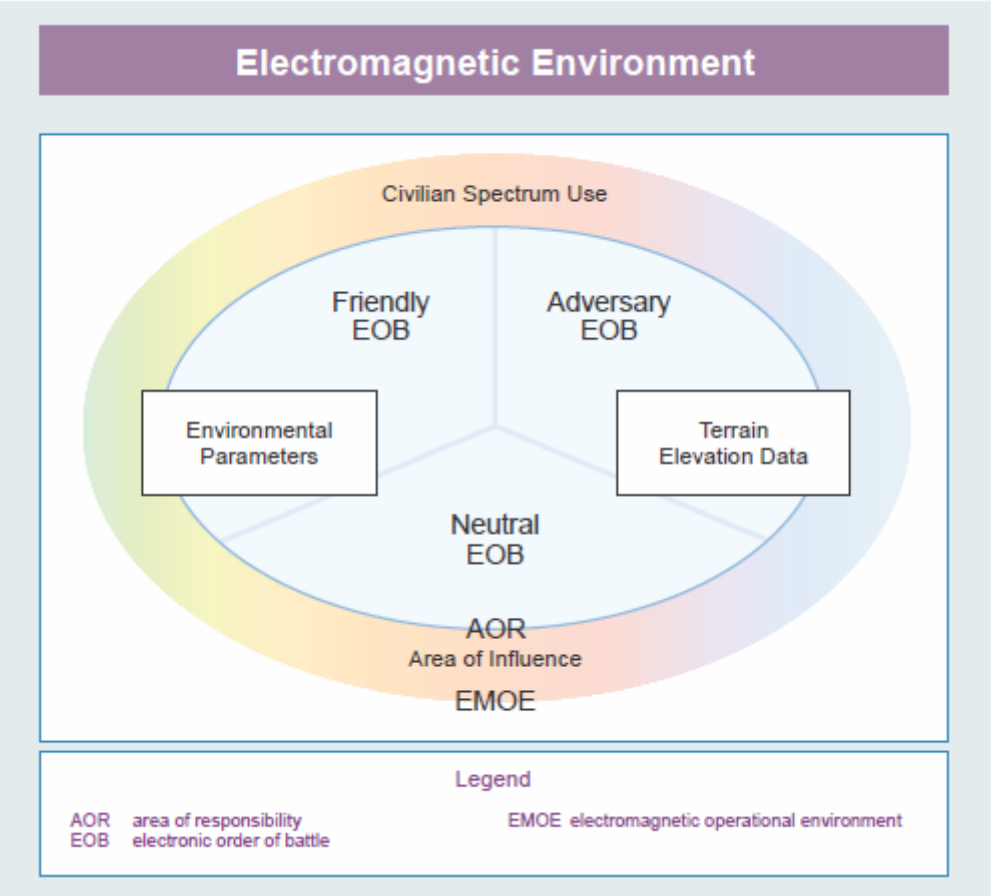

Figure 5. Electromagnetic Environment.

A. STRATEGIC PERSPECTIVE

The strategic priority for the RSNF has been keeping the SLOCs open through the Arabian Gulf and the Strait of Hormuz. These locations are vital for oil exports. All planning in any military is carried out in accordance with the commander's concept of operation, higher political level directives and grand, national military strategy.

Based upon strategic priorities and grand strategy the RSNF is organized on the "fleet in being" strategy. This strategy seems a good choice for the RSNF based on its fleet size and capability.

The "fleet in being" strategy employs the avoidance of direct confrontation with a superior enemy and focuses on preserving its own maritime assets. In short, the concept

of "fleet in being" is where one tries to remain viable until the end of hostilities and therefore continues to pose a threat to an adversary by interdicting targets of opportunity. In the twentieth century, the most obvious example of the conduct of a "fleet in being" strategy was that adopted by Germany through most of the First World War when, by keeping their major surface combatants away from decisive battle, they kept the British fleet tied down [25].

The Kingdom of Saudi Arabia does not have any offensive plans against any neighbor or regional state. Therefore, the entire force structure of the kingdom is based on its defensive needs and regional policing requirements.

B. OPERATIONAL PERSPECTIVE

The conduct of maritime operations has undergone transformation with changes in the geo-strategic and political environment worldwide. The end of the Cold War and consequent mitigation of threats of general and limited wars have shifted the focus of the navies away from the military role; the benign/constabulary tasks are becoming more predominant. In this changing environment, the RSNF is no exception. The Coalition Maritime Campaign Plan (CMCP) and Combined Task Force 150 (CTF 150) are manifestations of these new challenges.

The CMCP is a coalition force consisting of ships from major navies of the world. This coalition force is working to prevent terrorist attacks against vital maritime infrastructures in the Gulf region. International terrorist organizations pose a real threat to critical maritime infrastructures in the region, including the oil and shipping industries. Another important responsibility of the CMCP is to check and interrupt the trafficking of drugs, arms and humans. Similarly, CTF 150 is a multinational coalition naval task force having its headquarters in Bahrain. The task force's mission is to monitor, inspect, board and stop suspect shipping. All of these operations fall under the umbrella of Maritime Security Operations (MSO).

The primary mission of the RSNF during peace time will be performed in either a constabulary or a benign role. These roles are derived from the RSNF mission statement, which states that "Saudi naval forces play economic Facilities Protection tasks at sea and

in the protection of commercial, military, and civil convoys and securing the country's exports and imports in addition to assisting civil authorities in evacuation and rescue operations during disasters and crises" (Commodore Ali Alshehri, personnel communication, 2013). It can also be deduced that the RSNF will be employed in a self-defense posture in case of war.

C. CURRENT RSNF EW CAPABILITY

Three Al Riyadh (F3000S) class multipurpose anti-air warfare stealth frigates serve as the mainstay of the RSNF. These ships were built by DCNS of France. Al Riyadh class ships have some additional anti-air warfare and anti-submarine capability as compared to the French La Fayette class frigate upon which they are loosely based. The onboard electronic warfare suite includes the DR 3000 for ESM, the Altesse communications intercept system, the Salamandre B2 radar jammer, TRC 281 communications jammer and two Sagem Défense Sécurité Dagaie decoy launchers [26]. The Altesse integrates direction finding, analysis and interception functions to minimize processing time. The Altesse can operate in either the automatic scan, recurrent surveillance or fixed frequency mode [27]. The RSNF also operates Dauphin helicopters having ASE(2) electronic warfare suites onboard.

Saudi Arabia is in the process of establishing a national-level command, control, communications, computers and intelligence (C4I) system. Raytheon Network Centric Systems was awarded a $600M contract in 2012 to develop and deploy this system for the Kingdom. This modern C4I system is expected to link to the Kingdom's ground radar network. Moreover, the system will help to fuse information from advanced Royal Saudi Air Force (RSAF) surveillance assets, such as the E-3/RE-3 and Saab Erieye turboprop air borne early warning and control (AEW&C), to compile the tactical picture in real time jointly. The RSAF can effectively use all this information to command their advanced fighter fleets of F-15s, Eurofighters, and Tornados effectively [28]. Integration of naval EW assets in this overall C4I system is a priority operational requirement and is being handled accordingly.

D. ONGOING PROJECTS

As highlighted earlier, RSNF is undergoing an upgrade. This upgrade involves the acquisition of new platforms as well as modern weapons and systems. The ongoing projects that will directly affect EW capability are summarized below.

1. C4I

The Saudi Navy C4I system is unable to support effective modern combat operations on its own. This fact was realized practically when the Gulf War began. As a result, the Saudi Navy purchased a $307 million upgrade of its C4I system on September 27, 1990 [29]. Since that time, the Saudi Navy C4I has been upgraded significantly. It now has Link 16 secure communications capability, and its C4I/BM links are fully compatible with those of the U.S. Navy. RSNF manpower overall training proficiency and readiness have also been augmented to support complex combat operations. (Saudi Arabia Enters the 21st Century [30].

The RSNF C3 upgrade was a public project and proposals were solicited on the U.S. government procurement website Fed Biz Opps in 2003 [31].

In fact, the RSNF C4I system is a segment of the national level C4I system (The Peace Shield) managed by RSAF. The Peace Shield system links the networks of the Royal Saudi Land Forces (RSLF), RSNF and Royal Saudi Air Defense Force (RSADF). The Peace Shield program provides a nationwide ground-air defense and command, control and communications system to the RSAF. The Peace Shield mainly consists of 17 radars, a central command operations center, five sector command and operations centers, nationwide communications links, interfaces with all agencies having a role in national defense and communications centers to contact and control civil and military aircraft. The central command operation center is in Riyadh, while sector command and operations centers are located in Dhahran, Taif, Tabuk, Khamis Mushait and AI Kharj. The system includes 164 sites and more than 1,600 communications circuits [32].

Peace Shield integrates all long-range radar, remote-controlled air and ground radio communications sites and the associated telecommunications network. Data from the long-range 3D radars and tactical radars is fed into the Peace Shield. This system can

exchange data with airborne warning and control system (AWACS) ground entry stations, ECM-resistant ground-based 3D radars, integrated air defense missile systems, satellite communications (SATCOM), RSAF headquarters, air traffic/early warning radar sites located throughout the Kingdom and the radars of the RSNF. Peace Shield employs a secure high-speed broadband Wide-Area Network (WAN) to support the increased data exchange requirements of the entire C4I System. A High-Speed Network (HSN) is the communications backbone of the Peace Shield [33].

As highlighted earlier, the C4I project is a national project. It includes hardware and cyber security components. All C4I projects will integrate all sensors together to compile a real-time tactical picture of threats in areas of operation. All data from distantly located sensors will be fused together to generate a joint picture of the tactical situation at the national level as well as at command levels. It may be relevant to mention that details regarding current status, capabilities, any maintenance or operational issues, upgrade plans and cyber security of these C4I projects are not publically available due to security sensitivities. However, it is an established fact that the system is maintained and upgraded regularly to meet national air defense and EW requirements.

2. Saudi Naval Expansion Program-II (SNEP-II)

The RSNF is currently in the planning phase of the Saudi Naval Expansion Program-II (SNEP-II). The SNEP-II program is expected to include surface warships with integrated air and missile defenses, helicopters, patrol craft and shore infrastructure. This program is part of the Kingdom’s naval buildup to counter Iranian threats, particularly asymmetric and air threats.

The RSNF seems interested in the U.S. Littoral Combat Ship (LCS) armed with Lockheed Martin’s Aegis air-defense system. Lockheed, with a proposed multi-mission version of its fast new LCS, Australia's Austal, Ltd. and General Dynamics Corporation are in competition for provisioning the LCS-type surface vessels. The RSNF may select the same design as the U.S. or it may customize a few design features to meet its operational requirement. The RSNF is interested in systems offered with ballistic missile defense capability due to Iranian ballistic missile threat. LCS ships can be configured for

any role by changing the relevant modules [34]. Induction of the LCS into the RSNF will provide leverage for meeting diverse operational requirements with a minimal number of platforms, including missile and Anti Air Warfare (AAW) defense capability. Moreover, remotely operated vehicles can provide significant EW advantages with their extended range and mobility.

The RSNF has not yet finalized its weapons and sensors suite requirements as acquisition of the LCS is still in the planning phase. However, the LCS can be fitted with a naval forward-looking infrared radar, the Raytheon SeaRAM anti-ship missile defense system, three super rapid bloom of chaff (SRBOC) and two Nulka decoy launchers. The countermeasures suite may include ES 3601 tactical radar ESM from EDO Corporation. The LCS may also be equipped with Northrop Grumman Electronic Systems' integrated combat management system (ICMS), BAE Systems Electronic Systems' radio communications system and CAE Marine Systems' automated ship control system. The Link 16, Link 1, CEC, and Sea Giraffe radar can be installed on the main mast [35]. Inclusion of the LCS in the RSNF surface fleet will increase her EW capabilities, especially ECM, due to the availability of three SRBOCs and two Nulka decoy launchers. This decoy system will also play a vital role in overall missile defense capability for the fleet.

E. THREAT ANALYSIS

Saudi Arabia feels threatened by Iran's nuclear aspirations. Other regional states in the Middle East are also apprehensive about a nuclear-armed Iran. Iran has always portrayed herself as the guardian of Shiite Muslims all over the world. This image of Iran has emerged more clearly since the 1979 revolution. Therefore, Saudi Arabia along with other regional states, fears that a nuclear-armed Iran would destabilize already fragile Shiite-Sunni relations in the region. Shiite populations in mostly Sunni dominated states may resort to violent means for regime change with the help of Iran. The Bahrain unrest during the Arab Spring was indicative of this phenomenon. Open involvement of Iran in supporting the Shiite regime in Syria's ongoing conflict further supports this theme. Moreover, Iran's strategic location on the Arabian Gulf and the Strait of Hormuz may

provoke a disruption to oil supplies for a limited period of time. This may have a devastating impact for the local as well as the global economy [36].

Saudi Arabia does not feel threatened immediately by Israel's military upgrades due to the U.S. presence in the region and her strong ties with Saudi Arabia. This said, there is a diverging perception on the Palestine issue between the two allies. Saudi Arabia has a clear stance that Israel has to withdraw from the Palestinian territories occupied during and since the 1967 Arab-Israeli war. At present, Israel does not appear willing to yield to these demands. All Arab states including Saudi Arabia, therefore, have a sense of insecurity with regard to Israel, and this remains a point of contention between the U.S. and Saudi Arabia as well as other Arab states. Saudi Arabia cannot be fully assured that the U.S. will in all cases restrain Israeli aggression within the region, as the U.S. tries to balance the concerns of allies who are not themselves allies of each other. Therefore, Saudi Arabia must be concerned with any capabilities that Israel could bring to bear upon the Kingdom.

The RSNF plan for acquiring EW capabilities may be focused on collecting electronic and signal intelligence to counter the threats posed by both Iran and Israel. The EW capabilities of Iran and Israel are included as Appendix 1 and Appendix 2, respectively.

Iranian military doctrine is designed to target its adversaries' economic, political and military interests. Iran has publicly threatened to use its naval forces to close the Strait of Hormuz in response to increasing sanctions and in the event Iran is attacked. Iran has the capability to launch missiles against U.S. interests and her allies in the region in response to any attack by the U.S., NATO or any U.S. allies. Moreover, Iran's unconventional forces are well trained and present a formidable threat in the region. Iran continues to develop technological capabilities applicable to nuclear weapons and ballistic missiles that could be adapted to deliver nuclear weapons. Iran's ballistic missiles program with an extended-range variant of the Shahab-3 poses a continuous threat to her regional adversaries [37].

The Iranian Navy has aspirations of becoming a “blue water” navy. The Iranian Navy currently consists of three Kilo class submarines from Russia, 10 Houdong fast attack craft from China, domestically produced light submarine or swimmer delivery vehicles of various classes, naval aviation assets like the Mi-8 AMT (Mi-171) transport/attack helicopters, anti-ship sea skimming missiles equipped with modern anti-ship missiles, guided missile frigates and modern destroyers. Iran is also acquiring new deployment capabilities to strike against warships in the Persian Gulf in the case of an armed conflict.

Ever expanding Iranian naval capabilities are viewed in Riyadh with great concern. Iran has adequate naval strength to disrupt the smooth flow of oil supplies through the Strait of Hormuz in case of any conflict at least for a limited time. Any disruption in the smooth flow of oil supplies has a significant economic impact on Saudi Arabia. Many inbound imports vital for sustaining economic growth will also be threatened by any hostilities in the strait. It is matter of survival for the Kingdom and hence the RSNF to defeat any hegemonic designs focused against the Kingdom’s interests.

It is interesting to note that Israel and Saudi Arabia have a mutual potential adversary, Iran, and a mutual ally, the United States. However, the phrase, the enemy of your enemy is your friend, does not fit well in this case. Despite having a common adversary and a common friend, Saudi Arabia still feels threatened by Israel. However, it is also a relevant fact that development of force structure is normally aligned to deter the imminent threat due to high costs of modern sophisticated sensors and limited resources available at the discretion of the military leadership in developing countries like Saudi Arabia. SNEP II seems more aligned to counter the Iranian threat rather than the Israeli one. Selection of any sensor for acquisition or upgrade in future will, therefore, be dependent on this looming threat.

F. GAP ANALYSIS

This capability gap analysis is aimed at exploring technological advances in the EW field to identify areas in need of improvement and to obtain the best future EW capability, offering the best performance at an affordable cost.

Naval forces are organized to gain control of the sea in any event of hostilities to ensure the safety of national interests. Attainment of sea control is, therefore, the focal consideration of all maritime operations. Without it, no maritime operation—whether it is protection of a high value unit (HVU) in the escort role or power projection ashore—can be successful. While no single maritime military element can perform this job, naval warships in modern day naval warfare can be better equipped apart from having inherent essentials of poise, sustained reach, and resilience for establishment and maintenance of sea control. Effective control of the electromagnetic environment (EME) with the help of EW technologies can be a force multiplier. Moreover, effective EW assets guard the fleet against any sophisticated threats in the form of electronic disruptions and jamming under an overall environment of network centric warfare (NCW).

Protection of shipping and keeping the SLOCs open for vital petroleum, oil, lubricants (POL) supplies and maritime trade will be the primary mission of RSNF during hostilities. Effective protection of SLOCs can be ensured by deterring the attacks by enemy forces. To perform her mission effectively, rapid fusion of intelligence data from air, ground and surface sources will be required. This, in turn, is linked with C4I system capability to support such fusion and the technology of EW sensors and sensor platforms.

Another aspect which needs to be considered during the analysis is the power of the purse. The RSNF has found it prudent in past decades to modernize its fleet continuously and to acquire advanced weapons and sensors. But this may not be the case anymore. The Arab Spring has turned the tide and, hence, the priorities of national leadership. Future increases in population will require allocating considerable resources to meet domestic needs, such as education, housing and medical services, leaving behind fewer funds available for the acquisition of weapons and sensors.

G. RSNF ONBOARD EW ASSETS

Deployment of EW assets is governed by the commander's overall CONOPS. As highlighted earlier, RSNF does not have any aggressive designs. Although EW is a broad term that includes EA or ECM, ES or ESM and EP or ECCM, the RSNF has heavily invested in EW to be used in defensive measures. Table 1 summarizes KSA EW assets.

Name	Sensors
RSNF 4 x Madina Class FFG Madina Hofouf Abha Taif	ESM: Thomson CSF DR 4000 intercept ECM: Thomson CSF Janet Combat Data sys: Vega system 3CSEE Radars: Air/Surf/IFF: Thomson CSF sea Tiger (DRBV 15) Nav: 2 Racal Decca TM 1226 FC: Thomson CSF Castor IIB/C Thomson DRBC 32 (for SAM)
RSNF 4 x Badr Class FSG (Corvettes) Badr Al Yarmook Hitten Tabuk	ESM: SLQ –32 (V) 1 Radar: Air: Lockhead SPS – 40B (320 Km) Surf: ISC Cardion SPS – 55 FC: Sperry Mk 92 (I/J Band)
RSNF 9 x Al Siddiq Class PCFG	ESM: SLQ –32 (V) 1 Radar: Surf: ISC Cardion SPS – 55

	FC: Sperry Mk 92 (I/J Band)
RSNF 3 x Arriyad class (Mod. La Fayette Class) (Type F-3000S)	ESM: Thomson CSF (DR 3000 S2) ECM: 2 CSEE Salamandre Radar: Air: Thomson CSF DRBV 26 C Jupiter II Surv/FC: Thomson CSF Arabel 3D FC: Thomson CSF Castor II UJ Nav: Racal Decca 1226
RSAF	10 AWACS ground entry stations Command, Control, Communications, Computer and Intelligence (C4I) System The High-Speed Network (HSN)
RSADF	17 AN/FPS-117 long-range radar 06 AN/TPS-43 tactical radars
RSLF	AN/TPS-43 radars Improved HAWK air defense missile system

Table 1. RSNF onboard EW assets.

H. CAPABILITY GAPS

It is the information age and military leaders are learning that "it takes a network to fight a network" [38]. Availability of the right information at the right time in the right format and provided to the right man has become a fundamental planning factor among security establishments. NCW and FORCEnet concepts have become necessary to react effectively to any crisis. Accurate future planning can save scarce funds that would be

wasted by acquiring any system that does not offer any additional capability in the foreseeable future.

The RSNF cannot continue to operate in isolation from continually developing technologies. As new technologies will keep coming online, interoperability and integration challenges within RSNF legacy systems and systems of other sister services will keep surfacing. The RSNF, therefore, will be required to attain the capability of effective integration of new systems with the old legacy systems.

The RSNF needs to bridge the following gaps in her capability to meet its EW mission requirements effectively. Some of the following factors listed may not directly affect EW capability, but they have a relationship with efficacy of EW systems when viewed from a national security perspective.

- Prevent HF/VHF radio communication interception
- Improve HF/VHF/UHF DF capability
- Prevent HF/VHF radio spectrum selective jamming
- Prevent interception of microwave, troposcatter and satellite communication
- Prevent interception of all kinds of data transmission, FAX and emails
- Cyber Warfare (Logic bomb, microbe, etc.) defense against our communication systems (PASCOM, DEFCOM, PATCOMS and SATCOM)
- ESM and ECM against non-communication emitters (i.e., radars and radar guided weapon systems)
- Limited code breaking/decryption of encrypted voice and data transmission
- Short duration electronic deception in a selected sector
- Improved "jointness" with RSAF, Royal Saudi Air Defense Forces (RSADF), RSNG and RSLF in a variety of defense missions
- Develop true interoperability with sister services and allied nations, especially the U.S., UK, France and GCC naval forces with respect to electronic intelligence gathering and sharing
- Improved coastal defense capability through the installation and integration of new ESM and ELINT sensors along the coast

- Improved training standards in C4I, IT and EW fields, especially in the eastern fleet command
- Improved ballistic missile defense (BMD)
- Upgraded AWACS for better jointness, better ELINT/EW and maritime patrol aircraft (MPA) functioning
- Improved netting and identification friend or foe (IFF) with RSAF, RSNG, RSADF, RSLF, U.S. Air Force, U.S. Navy, GCC air forces, Saudi and GCC land-based air defenses

V. CURRENT TECHNOLOGICAL TRENDS

Technology is changing at a very fast pace. Military establishments find it more challenging to keep pace with advancing technology in every field. Switching cost from one technology to another in the military technology domain is very expensive. Military planners, therefore, dedicate considerable effort to monitoring current technological trends and updating their acquisition plans based on capability gap analysis in light of these ongoing trends.

Military operations are becoming more complex in nature due to the doctrinal shift from conventional warfare to asymmetric warfare. Added complexity in combat operation will demand more technological support at the lowest level of force structure. Although EW planning and EW operations are conducted at higher organization levels, this doctrinal shift has still impacted current technological trends in EW. Current trends in the EW domain encompass electro-optical warfare, use of microprocessor based systems, elevated platforms, jam-proof radars, employment of satellites and analysis equipment.

Being a very expensive technology, most of the developments in EW have taken place only in a few leading countries and organizations including America, Russia, China and NATO countries, which provide the role model for others to follow. KSA is in the process of acquiring state-of-the-art EW equipment in the pursuit of safeguarding her command and control structure from potential threats by the regional countries. To maintain its operational readiness and effectiveness, RSNF is bound to take suitable measures by improving her EW capabilities and maturing her concepts, doctrines and organizations in light of new challenges vis-a-vis available and affordable technology.

A. REGIONAL TRENDS

1. United States of America

The U.S. military began its efforts to combine the tactics of EW with intelligence, deception, surprise, command and control, electronic suppression and electronic protection in late 1960s. The Army doctrine has been geared towards gathering signals

intelligence and also towards wrecking the enemy's command, control, communication and intelligence systems. The Air Force doctrine is intended to disrupt the enemy's air defense systems of radars, fighters and missiles. The Navy doctrine is focused on allowing the Navy to get off the first effective in any engagement while wrecking an enemy's sensors and communications. The Department of Defense (DoD) spends an enormous amount every year on highly classified "Black Programs."

2. Russia

The Russian military doctrine for the use of the electromagnetic spectrum is called radioelektronnaya bor'ba (REB), which is translated as radio-electronic struggle. Russians combine the tactics of EW, surprise, deception and fire power to create to a unique doctrine that shapes the operation of the Russian Army. REB includes the actions to disrupt an enemy's use of the spectrum and actions to protect friendly use of the spectrum. It incorporates razvedka (reconnaissance and intelligence) and maskirovka (concealment and deception). In peace time REB is intended to help conceal Russian military capabilities, deceive Western intelligence analysts and acquire training for war and low intensity conflicts. In war time its mission is to paralyze enemy command, control and communication and protect friendly use of the spectrum. After the downfall of the Soviet Union the doctrine of the REB shifted from offensive to defensive in nature. Russian definition of defensive sufficiency intends to reduce its military forces to the minimum required for reliable defense of the motherland. REB operates in close cooperation with KGB. Its scope includes radio, radio technical, radar, electro-optical, radio-thermal, laser, television, acoustic and hydro-acoustic intelligence.

3. North Atlantic Treaty Organization (NATO)

The NATO Electronic Warfare Advisory Committee (NEWAC) was established in 1966 to support the Military Committee, the NATO Strategic Commanders and member nations by acting as a joint, multinational body to promote an effective NATO EW capability. It monitors progress achieved nationally and within the Integrated Military Command Structure in implementing agreed EW measures. It is responsible for the development of NATO's EW policy, doctrine, operations and educational

requirements and contributes to the development of command and control concepts. Electronic warfare capabilities are a key factor in the protection of military forces and in monitoring compliance with international agreements and are essential for peacekeeping and other tasks undertaken by the Alliance. NEWAC also assists in introducing NATO's EW concepts to partner countries in the framework of Partnership for Peace.

4. China

China has developed the idea of Special Operation Forces (SOF) to combat EW. Since 1997, SOFs (Quantou Budui, fist units) have carried out many EW missions at the national and international level. During the same period, Chinese companies began to market man-portable EW systems, suitable for employment by SOF against C2 facilities. The People's Liberation Army's (PLA) definition of EW includes physical attacks on the full range of command, control, communications, computers, intelligence, sensors and reconnaissance (C4ISR) systems and networks. In fact, the terms EW and information warfare (IW) seem to be used almost interchangeably by the PLA. Ground-based EW systems have a limited range due to propagation losses, terrain masking and other obstacles. SOF teams are employed by ground, air or naval means to infiltrate the enemy's operational and strategic depth. In addition to traditional EW actions, Chinese authorities have begun to comment on the possibility of using special operations to attack automated command networks.

B. MODERN TECHNOLOGICAL TRENDS IN EW

The primary reason why EW is becoming more and more complicated is because defenders have learned how to adapt to various EW strategies. Radars have become more powerful, more discriminating and more agile. Command and control networks have become more resilient and responsive. Surface-to-Air missiles have become smarter. Improvements in aircraft radar and radar-guided air-to-air missiles allow for longer-range engagements of multiple aircrafts and have pushed the aerial engagement arena well beyond visual range (BVR). Vastly improvised infrared (IR) guided missiles are now capable of head on, high-angle, off-foresight engagement that give no indication to the target.

New technologies such as data fusion are emerging to provide an overall picture of information from a variety of active and passive sensors. There is an increasing use of lasers for both protection and offense. Ongoing technological trends in EW can be organized in three areas..

C. NEW TRENDS IN ESM

The telescope was the first passive information instrument. Since then tremendous breakthroughs in the area of combat identification have been made and are still attracting most attention. However, the key to ESM systems or what separates the leading ESM systems from the second string is the database. Database storage capacity and its ability to carry out all the parametric analysis of all signals that are likely to be encountered. The information about these technologies in the following sections has been gathered from Internet, global security websites, military technology websites, *Jane's Defense Weekly*, *Jane's Defense Fighting Ships*, and Gulf military balance 2011 report.

1. Acousto-Optic

Acousto-Optic receivers with their advantages of wide instantaneous coverage of the entire band are becoming increasingly popular. An improved acousto-optic radar warning receiver will provide faster and more accurate warning of hostile radar activity. Optical signal processing techniques allow the receiver to simultaneously handle a wide range of frequencies and analyze several signals in parallel while providing frequency resolution precise enough to separate hostile signals from friendly ones.

2. Improvement in Antenna Design

One major breakthrough in the ESM technology is the improved antenna design. The antenna design widely depends on the type of ESM equipment and the platform on which they are mounted. For obvious reasons, aircraft antennas have to be small and lightweight and consequently provide less facility than the ground-based or ship-borne systems. For the latter applications, a wide variety of passive and active dipoles and DF antennas, both directional and omni-directional are employed. Submarines have a

particular need for antennas that give the least possible radar cross-section to avoid detection and are sufficiently compact to be mounted in the restricted space on the sail.

D. NEW TRENDS IN ELECTRONIC COUNTERMEASURES

In the future, there will be a great many more smart weapons and as these systems are widely proliferated, we will find it much more difficult to counter them.

1. Missile-Borne ECM Technology

The Missile-Borne ECM Technology (MBET) program is a comprehensive program designed to provide critical information to decision-makers and others regarding the ability of modern Air and Missile Defense systems to engage and destroy an adversary's Tactical Ballistic Missile (TBM) in the presence of missile-borne ECM. An outgrowth of the MBET program is the Tactical Ballistic Missile-Borne Jammer (TBMBJ), which is the first demonstration of a Threat-level ECM device being integrated into a Threat-representative target while maintaining full capability of the target delivery system.

2. Advanced Electronic Countermeasures (ECM) Pod

The ALQ-131 is an advanced ECM pod designed to provide an aircraft self-protection against radar threats. The ALQ-131 accomplishes this by responding with a combination of noise, repeater or transponder electronic jamming techniques. The pod weighs 600 pounds, with modular design for multiple frequency band capability. It has an ability to be quickly re-programmed against changing threats. The present TBMBJ system is a responsive frequency-agile system capable of producing a wide range of threat-representative ECM waveforms. With simple electronic module changes, the system can be made to produce any number of different ECM waveforms. With simple programmable changes, the system has the ability to transmit any of these waveforms in several modes to include barrage, blinking and responsive.

3. Advanced Airborne Expendable Decoy (AAED)

AAED is a towed expendable intended to provide a radar target decoy to an incoming missile. The AAED can be manually operated as a stand-alone device, or it can be integrated and controlled by the ALE-47. This expendable towed decoy is designed to provide countermeasures against radar guided anti-aircraft threats, thereby increasing the survivability of tactical aircraft. The decoy is deployed when required and cut free before landing. The program is in the full rate production (FRP) phase.

4. Laser Based Decoys

The latest generation of Anti-Missile ECM use laser-based transmitters to create multiple lines of decoy energy in the missile bands. Perhaps this class of system, used in conjunction with closed loop infrared counter measures (IRCM) and flares, will buy some time against the truly imaging-seeker threats coming down the road.

5. UAVs

Many countries worldwide are employing Reconnaissance, Intelligence, Surveillance and Target Acquisition (RISTA) systems for the detection and location of targets. Unmanned Aerial Vehicles (UAVs) will conduct RISTA against tactical and operational targets throughout the theatre. UAVs include drones, characterized by pre-programmed flight paths and patterns, and remotely piloted vehicles (RPVs). Each can perform a variety of missions, ranging from reconnaissance and surveillance to attack and electronic warfare.

In addition to information gathering (still the dominant function), UAV roles will include electronic combat, decoy, ground attack, and suppression of enemy air defense (SEAD). A significant new capability involves the direct linkage of a reconnaissance UAV to a fire direction center. This linkage provides real-time information to commanders, followed by immediate fire and damage assessment. UAVs are also good candidates for stealth technology and spin-off technologies from Cruise Missiles (CM) developmental programs. The X-47B stealth drone is set to be the world's first unmanned, robot aircraft piloted by artificial intelligence rather than a remote human operator. The

program is currently in the engineering, manufacturing and development (EMD) phase. Another program also in the EMD phase is that of the unmanned jet MQ-4C Triton which is capable of flying 11,500 miles without refueling. The MQ-4C will be used for high altitude maritime surveillance. Successful induction of the X-47B drone and MQ-4C unmanned jet in the U.S. Navy will revolutionize the role of the drone in naval warfare due to their extended range.

E. NEW TRENDS IN ELECTRONIC COUNTER – COUNTER MEASURES

1. Millimetric Frequencies

There is a growing tendency to shift the frequency coverage of electronic warfare beyond the radar and communication frequencies to cover great areas of the spectrum. New threats based on millimetric wave radar and electro-optical guidance have already spurred the development of EW hardware able to cover these frequencies. Radar frequencies in the 35 GHz and 94 GHz windows, which are above the conventional radar band, were used in the Gulf War.

2. Passive Surveillance Systems

A great deal of development effort has recently gone into the use of passive surveillance systems for detection. These are either optical or infrared in design and, because they do not transmit, are not vulnerable to anti-radiation missiles. They are, however, very limited in range and are still vulnerable to infrared or optically guided missiles. A number of the latter type has been in operational use for some years, using a television camera in the nose. The defense against these is normally to use a smoke screen and several systems, which combine the deployment of smoke, chaff and infrared flares currently in use.

3. Multi-Static Radar for Improved and Stealth Detection

In order to survive and do their job, radar stations of the future will have to be difficult to attack with guided missiles or to jam electronically. They must also be capable of detecting objects, which use stealth technology. Radar manufacturers are

working on multi-static radar, with transmitters and receivers separated geographically, as one of a number of solutions to survivability and performance.

4. Smart Skin (No Antenna)

An average modern fighter has no fewer than 30-35 RF antennas distributed over its surface, performing functions such as communications, navigation, identification, threat warning, active jamming and target detection. There are so many of them that their size is to be kept to a minimum to cater for aerodynamics, drag, low radar cross section (RCS) and weight considerations, which in most cases leads to a compromise in performance. The U.S. Air Force has been working on this problem since the early 1980s and has been able to design, construct and test an embedded wide-band antenna, a so-called "Smart Skin." Not only are these antennas large, but they also have steerable beams for much higher performance than conventional antennas. Japan has recently tested a smart skin phased-array antenna for aircraft.

5. Integrated Defensive Electronic Countermeasures (IDECM)

The IDECM system is a radio frequency, self-protection electronic countermeasure suite resident on F/A-18 aircraft. The system is comprised of onboard and off-board components. The onboard components receive and process radar signals and can employ onboard and/or off-board jamming components in response to identified threats. IDECM Block-3 is currently in the full rate production phase. There are four IDECM variants: Block I (IB-1), Block II (IB-2), Block III (IB-3), and Block IV (IB-4).

F. THE WAY FORWARD FOR RSNF

Services all over the world are facing new challenges in an uncertain and dynamic global environment. Forces need to leverage innovative concepts, cutting-edge technologies, and joint-integrated operations to meet current and future challenges effectively and economically. RSNF cannot blindly follow the footsteps of leading navies of the world, especially in the acquisition of EW systems. The basic and foremost reason is that there are vast differences in existing weapons and sensors infrastructure. The U.S. Navy, NATO, China and India have legacy systems as per their peculiar

security and integration requirements. Full integration of newly acquired systems with old legacy systems is a very basic consideration for RSNF future planners. KSA does not have any impressive capability in the field of integration. Due to a very thin in-house defense manufacturing industry, systems in service are of different origins, having different interface protocols. RSNF, therefore, needs to analyze structural, organizational, doctrinal, training, supportability, maintainability and logistical issues along with operational requirements. After due deliberation on all these aspects, RSNF is expected to have few feasible options.

RSNF is a regional force and has a limited scope of operation without any offensive design. The essential requirements of EW systems vary from those of leading navies because of their quest for global presence versus the RSNF posture of a regional defensive force. Any system in service with leading navies may not be cost effective for the RSNF because of high acquisition costs and subsequent life cycle costs for maintenance and operation.

Saudi Arabia is one of the 10 largest defense systems and equipment markets worldwide. Superior EW systems enhance the survivability of highly expensive surface platforms. Since naval systems upgrades and modernization programs are less expensive than overall platform replacement, selection of affordable technological advancements will play a key role for enhancing existing EW systems capabilities.

As per the global EW system market report 2012- 2022, the United States represents a major market for EW systems. Defense equipment manufacturers are expected to produce thousands of EW systems such as ECM systems, ESM systems, and radar warning receivers (RWRs). The production rate is expected to rise significantly over a period of ten years, driven by the increased demand from military forces and the increasing danger across the global waterways [39]. As a result, the price of EW systems may go down due to economies of scale. RSNF may, therefore, delay acquisitions of EW systems where possible to leverage the benefit of mass production.

Lockheed Martin, BAE Systems, Boeing, Northrop Grumman, General Dynamics and Raytheon are the leading global defense suppliers. U.S.-centric defense suppliers

include Alliant Techsystems, Inc., Communications & Power Industries, DRS Technologies, General Dynamics Corporation, ITT Corporation, L-3 Communications Corporation, Lockheed Martin Corporation, Northrop Grumman Corporation, Raytheon Company, Rockwell Collins, SRA International, and The Boeing Company. RSNF may establish a committee composed of officers from EW, acquisition, logistics and headquarters staff to visit these firms' facilities and evaluate the systems being manufactured.

Booz Allen Hamilton has recently been registered by the KSA Ministry of Commerce and Industry to pursue business opportunities in the Kingdom in support of domestic economic diversification. The firm has also been assisting the RSNF for more than three decades now. Booz Allen is a world leader in the area of intelligence-based cyber security along with management services experience. The firm is also being awarded a contract as part of SNEP including support for electronic warfare. RSNF may capitalize on the firm's expertise to short list EW systems best suited for RSNF operational requirements.

The association of old crows (AOC) is an independent, nonprofit, international professional association promoting public understanding in the science and practice of EW, SIGINT and related disciplines. The AOC is working with the King Abdulaziz City for Science and Technology (KACST) to organize the third Saudi Arabian EW Symposium in November, 2013. Delegates of leading EW systems manufacturing firms will be attending and exhibiting their products and literature. RSNF may nominate a team of officers from the operations branch with EW specialization and representatives from EW Directorate RSNF Headquarters to attend this symposium. This will help them learn about the current EW capabilities of the international electronic warfare industry and latest developments in thinking, products and services in EW.

BAE Systems has been recently been awarded a contract for upgrading 70 state-of-the-art Digital Electronic Warfare Systems (DEWS)/Common Missile Warning Systems (CMWS) onboard F-15S fighter jets by the RSAF. The work is expected to be completed by 2018. RSNF may consult RSAF authorities for learning from their experience and can negotiate its requirements with BAE systems. This arrangement will

not only save money but will help in the longer term from the integration, logistic support, standardization, maintenance, training and spare parts supportability perspective also.

Additionally, Advance Electronic Company (AEC) is a Saudi private sector company that serves the defense needs of the Kingdom. The AEC charter includes design, development, manufacturing, the provision of upgrades and logistical support of electronic products and systems. The firm has experience working on Electronic Warfare System ALG135EW and Radar Warning System ALR-56C RWR. RSNF may contract with AEC, and AEC may subcontract any of the jobs to the original equipment manufacturers (OEMs). AEC has a Military Systems Business Unit (MSBU) which has experience working on diverse major military programs in partnership with leading international OEMs. This arrangement will support the Saudiazation effort and long-term local technical and logistical support.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY AND CONCLUSION

Today there is a fundamental shift from conventional war fighting to the asymmetric nature of warfare. Militaries are more focused on conducting military operations short of war or military operations other than war. Ever deteriorating regional security in the Middle East and North Africa (MENA) demands a higher level of preparedness from the RSNF to meet any challenges that arise. EW equipment can help to prevent the situation from escalating beyond desired levels by providing a comprehensive and timely awareness of situations, so that politicians and commanders can determine appropriate reactions and implement them while the situation is still manageable. This can only be realized with the help of a very powerful infrastructure of electronic warfare facilities, robust command and control centers and extremely reliable communication channels.

The EW requirements of the RSNF vary from those of leading navies of the world because of the RSNF's posture as a regional defensive force. Any system in service with leading navies may not be cost-effective for RSNF because of high acquisition costs and subsequent life cycle costs for maintenance and operation. RSNF has to make tradeoffs between mission requirements and affordability. Naval systems upgrades and modernization programs are less expensive than overall platform replacement; selection of affordable technological upgrades for enhancing existing RSNF EW systems capabilities is a challenge for RSNF.

Saudi Arabia is progressing as an economic as well as a military power in the Middle East. The Royal Saudi Armed Forces in general and RSNF in particular shoulder a heavy responsibility for guarding national interests from any threat. This mission needs statement demands RSNF military hardware modernization. Integration of newly acquired systems with old legacy systems remains a basic consideration for RSNF due to a very thin in-house defense hardware manufacturing industrial base. KSA does not have any impressive capability in the field of integration. RSNF is, therefore, constrained to analyze structural, organizational, doctrinal, training, supportability, maintainability and

logistical issues along with operational requirements during the acquisition planning process.

At the same time, KSA needs to consider the way forward without too much delay. Saudi Arabia feels threatened by Iran's nuclear aspirations and Israel. Iran has always portrayed herself as the guardian of Shiite Muslims all over the world. Therefore, Saudi Arabia along with other regional states fears that a nuclear-armed Iran would destabilize the already fragile Shiite-Sunni relations in the region. These fears are supported by many of the current Iranian foreign policy moves in the international arena. The Bahrain unrest during the Arab Spring was indicative of this phenomenon. Open involvement by Iran in support of the Shiite regime in Syria's ongoing conflict further supports this theme. The Iranian missile program is another major concern, and the RSNF needs to prepare accordingly to face this threat.

Furthermore, while Saudi Arabia enjoys good relations with the U.S., there is a diverging perception of the Palestine issue between the two allies. Saudi Arabia has a clear stance that Israel has to withdraw from the Palestinian territories occupied during and since the 1967 Arab-Israeli war. However, Israel does not appear willing to yield to these demands. All Arab states including Saudi Arabia, therefore, have a sense of insecurity with regard to Israel, and this remains a point of contention between the U.S. and Saudi Arabia as well as other Arab states. Saudi Arabia cannot be fully assured that the U.S. will in all cases restrain Israeli aggression within the region as the U.S. tries to balance the concerns of allies who are not themselves allies of each other. Therefore, Saudi Arabia must be concerned with any capabilities that Israel could bring to bear upon the Kingdom.

The RSNF is undergoing thorough modernization and extension programs. As new technologies are coming online, interoperability and integration challenges within RSNF legacy systems and systems of other sister services are becoming more prominent. Effective integration of these new systems with the legacy systems, sister services and interoperability with allied regional and extra regional forces is the biggest gap. The RSNF needs to bridge the gaps highlighted in Chapter IV to meet its EW mission requirements effectively.

As part of the modernization and upgrade programs, KSA is in the process of acquiring state-of-the-art EW equipment which is a solid step forward. To maintain its operational readiness and effectiveness, RSNF is committed to take suitable measures by improving her EW capabilities and maturing her concepts, doctrines and organizations in the light of new challenges vis-a-vis available and affordable technology. Technological trends, leading EW systems manufacturers, available high tech systems and the way forward for the RSNF have been discussed in previous chapters to highlight the contours of a proposed RSNF acquisition strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. IRAN WE ASSETS

PLATFORM	SENSOR
3 x **Kilo** class (Type 877EKM)(SSK) • Tareq • Noor • Yunes	**ESM:** • Squid Head; radar warning. Quad Loop D/F **Radar:** • Surf : Snoop Tray MRP-25 (I band)
3 X **Alvand (Vosper Mk 5)** Class **(**FFG) • Alvand • Alborz • Sabalan	**ESM:** • Decca RDL 2ABC(radar warning) **Radar:** • Air/Surf: Plessey AWS 1(E/F band) • Surf : Racal Decca 1226 (I band) • Nav : Racal Decca 629 (I/J band) • FC : Contraves Sea Hunter
3 X **KAMAN (Combattane II**) (Fast Attack Craft)	**ESM** : • Thomson-CSF TMV 433 Dalia **Radar**: • Surf/ FC: Signaal WM28 (I/J band) • Nav : Racal Decca 1226 (I band)
3 X **THONDOR (HOUDONG**) (Fast Attack Craft)	**ESM**: • Thomson-CSF TMV 433 Dalia **Radar**: • Surf: China SR-47A (I band) • Nav: Rice Lamp Type 341(I/J band)
2 X BAYANDOR Class (Corvettes) • Bayandor • Naghdi	**Radar:** • Air/Surf: SPS – 6C(D band) • Surf : Racal Decca (I band) • Nav : Raytheon 1650 (I/J band) • FC: Western Electric Mk-36(I/J band)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. ISRAEL EW ASSETS

PLATFORM	SENSOR
3 x EILATH class missile corvettes • Eilat • Lahav • Hanit	**EW Suite & Decoys:** • Argon ST AN/SLQ-25 Nixie decoy • Elbit chaff rocket launchers • Rafael RF corner reflector • Elisra NS-9003A/9005 RWR **Radar:** • Elta EL/M-2218S air search radar • Elta EL/M-2221 fire-control radar
2 X Aliyah class FAC(M) • Aliya • Geula	**EW Suite & Decoys:** • Elbit chaff rocket launchers • Elisra NS-9003A/9005 RWR **Radar:** • Thales Neptune air & surface search radar • Selenia Orion fire-control radar
8 X Hetz class FAC (M) • Romach • Keshet • Hetz • Tarshish • Kidon • Yaffo • Herev • Sufa	**EW Suite & Decoys:** • Elbit chaff rocket launchers • Elisra NS-9003A/9005 RWR **Radar:** • Thales Neptune air & surface search radar • ELTA EL/M-2221 fire-control radar
3 X RESHEF class (Fast Attack Craft) Missile • Nitzachon • Atzmaut	**ESM**: • Nil **Radar**: • Surface/air search radar Neptune/S.P.S • Fire-control radar - Orion
5 x Dolphin class submarine • Dolphin • Livyathan • Tekumah	**EW**: • TIMNEX 4 CH ELINT/targeting set RWR/DF **Combat System**: • STN Atlas ISUS 90-55 combat system

• Tannin • Rahav	
2 x 707 ELINT 2 x 707 PHALCON AEW 3 x Beech KING AIR B200	• Cheek-antenna array • Radar, IFF, ESM/ELINT and CSM/COMINT • FLIR

EXPECTED THREATS

- Interception of our HF/VHF radio communication
- DF of HF/VHF/UHF
- Selective jamming of HF/VHF radio spectrum
- Interception of microwave, troposcatter and satellite communication
- Interception of all kinds of data transmission, FAX and e-mails
- Cyber Warfare (Logic bomb, microbe etc) against our communication system (PASCOM, DEFCOM, PATCOMS and SATCOM)
- ESM and ECM against non-communication emitters i.e. Radars and Radar guided weapon systems
- Limited code breaking/de-crypt ion of encrypted voice and data transmission
- Short duration electronic deception in a selected sector.

LIST OF REFERENCES

[1] Thomas W. Lippman, *Saudi Arabia on the Edge.* Potomac Books: Dulles, VA: 2012.

[2] Arif Sharif, Saudi Arabia Loans Growing Fastest in Persian Gulf: Arab Credit [Online]. Available: http://www.businessweek.com/news/2011-07-05/saudi-arabia-loans-growing-fastest-in-persian-gulf-arab-credit.html.

[3] Saudi Arabia: Political overview. [Online]. Available: http://news.bbc.co.uk/2/hi/middle_east/3784879.stm.

[4] Joseph A. Kechichian. *Legal and Political Reforms in Saudi Arabia.* Routledge Taylor & Francis Group: New York, 2013, p. 212.

[5] CIA Factbook. *Saudi Arabia* [Online]. Available: https://www.cia.gov/library/publications/the-world-factbook/geos/sa.html.

[6] Library of Congress, Federal Research Division. (2006, Sep.) Saudi Arabia economy profile. [Online] accessed on http://www.indexmundi.com/saudi_arabia/economy_profile.html.

[7] Abbas Kadim et al., eds., *Governance in the Middle East and North Africa, A Handbook.* Routledge: New York, 2013.

[8] U.S. Army EW doctrine FM 3-36. [Online]. Available: Army Knowledge Online https://armypubs.us.army.mil/doctrine/index.html.

[9] Organization of Islamic Countries, *about OIC* OIC) website [Online]. Available: http://www.oic-oci.org/oicv2/page/?p_id=52&p_ref=26&lan=en.

[10] Gal Luft. (2007). Dependence on Middle East energy and its impact on global security. [Online]. Available: http://www.iags.org/luft_dependence_on_middle_east_energy.pdf.

[11] Global Security Organization. Royal Saudi Naval Forces. Available: http://www.globalsecurity.org/military/world/gulf/rsnf.htm.

[12] Arabic Wikipedia. [Online]. Available: http://ar.wikipedia.org/wiki/القوات_البحرية_الملكية_السعودية)

[13] GAO Report 03-51. (2002, Nov.) Comprehensive strategy still needed for suppressing enemy air defenses. [Online]. Available: http://www.gao.gov/new.items/d0351.pdf.

[14] DoD joint operations Joint publication 3-0,2011. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

[15] DoD Electronic warfare Joint publication 3-13.1. 2007. [Online]. Available: http://www.fas.org/irp/doddir/dod/jp3-13-1.pdf.

[16] Anthony E. Spezio. "Electronic warfare systems," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, March 2002, p. 633.

[17] *IEEE Proceedings*, vol. 132, pt. F, no. 4, Jul. 1985. [Online.] Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04646598.

[18] PLC Training. Chapter 11, Countermeasures. [Online]. Available: http://www.fas.org/man/dod-101/navy/docs/fun/part11.htm

[19] Access Science. Jamming. [Online]. Available: http://www.accessscience.com/overflow.aspx?SearchInputText=Jamming&ContentTypeSelect=4.

[20] *Royal Navy's 'Radar Principles' Student Study Guide*, Royal Navy Maritime Warfare School, HMS Collingwood: London, 2004.

[21] Petter G. Forrest, *Telecommunication radar elctronic warfare 32254-80*, Labvolt: Canada,1999.

[22] Andrea De Martino, *Introduction to modern EW systems*. Artech House: Boston/London. 2012.

[23] Richard G. Wiley, *Interception and analysis of radar signals*. Artech House: Boston/London. 2006.

[24] Philip E Pace, *Detecting and classifying low probability of intercept radar*, 2nd edition. Artech house: Boston, 2009.

[25] *Fleet in Being*, [Online.] Available: http://www.globalsecurity.org/military/ops/fleet-in-being.htm .

[26] *Al Riyadh (F3000S Sawari II) Class, Saudi Arabia*, [Online.] Available: http://www.naval-technology.com/projects/al_riyadh/ .

[27] Norman Friedman, *Naval Institute Guide Book for Naval weapon Systems*, Annapolis Naval Institute press: 2006 p 346. [Online.] Available: http://books.google.com/books?id=4S3h8j_NEmkC&pg=PA346&lpg=PA346&dq=ELINT+SYSTEM+FITTED+ONBOARD+AL+RIYADH&source=bl&ots=hIYqKW2_d_&sig=MG0dfQL6k26jLzkF1qxUSRZ29XE&hl=en&sa=X&ei=Q_WsUYj8A6L0iQKNkoGwBA&sqi=2&ved=0CCoQ6AEwAA#v=onepage&q=ELINT%20SYSTEM%20FITTED%20ONBOARD%20AL%20RIYADH&f=false.

[28] Defense Industry Daily website, *Saudi Arabia Orders $600M+ National Command System* [Online] Available: http://www.defenseindustrydaily.com/Saudi-Arabia-Orders-600M-National-Command-System-07620/ .

[29] Richard F. Grimmett,,*Arms Sales to Saudi Arabia*, Congressional Research Service, IB91007Libraray of congress: Washington DC, 1991.

[30] Anthony H. Cordesman , *Saudi Arabia Enters the 21st Century: The Military and Internal Security Dimension*, Center for Strategic and International Studies: 2002. [Online] Available: http://csis.org/files/media/csis/pubs/saudimilbook_06.pdf.

[31] Fed Biz Opps website, *RSNF C3 Upgrade*. 2003 [Online] Available: https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=e6c16bd158206841a05c8b70a4d78294

[32] Defense PK website, *Saudi Arabia - Peace Shield* . [Online] Available: http://www.defence.pk/forums/arab-defence/242743-saudi-arabia-peace-shield.html#ixzz2aSvaQUH4)

[33] Global security website, *peace shield.* [Online.] Available: http://www.globalsecurity.org/military/world/gulf/sa-peace-shield.htm.

[34] Global security website, *Royal Saudi Naval Forces (RSNF) Modernization*. [Online] Available: http://www.globalsecurity.org/military/world/gulf/rsnf-modernization.htm.

[35] Naval Technology website, *LCS, United States of America*. [Online] Available: http://www.naval-technology.com/projects/littoral/.

[36] Shams-uz-zaman, *Implications of a nuclear-armed Iran on the Middle East and Pakistan.* [Online] Available: http://www.issi.org.pk/publication-files/1340000677_18060791.pdf.

[37] DoD, *Annual Report on Military Power of Iran*. [Online] Available: http://www.fas.org/man/eprint/dod-iran.pdf.

[38] Scott Jasper, *Transforming defense capabilities, new approaches for international security*, Lynne Reinner Publishers, Inc: Boulder Colorado, 2009.

[39] Global Industry Analysts, Inc website, *Electronic Warfare Systems: A US Market Report*, [Online] Available: http://www.prweb.com/releases/electronic_warfare_system/electronic_protection/prweb4209244.htm

Notes on personal communication

1. Commodore Ali Alshehri: Commodore Ali Alshehri was dean of education at King Fahad Naval Academy in 2008. He has a wide experience of serving in various command positions.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California